MobileView 9000 & 9100 Series Analog/IP Camera User Manual

P/N 1072868 • REV A • ISS 05NOV14

Copyright © 2014 United Technologies Corporation.

MobileView is part of UTC Building & Industrial Systems, a unit of United Technologies Corporation. All rights reserved.

Trademarks and patents The MobileView product name and logo are trademarks of United Technologies.

Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.

Manufacturer

UTC Building & Industrial Systems
4001 Fairview Industrial Dr. SE,
Salem, OR 97302, USA

Authorized EU manufacturing representative:
UTC Climate Controls & Security B.V.,
Kelvinstraat 7, 6003 DH Weert, Netherlands

Intended use Use this product only for the purpose it was designed for; refer to the data sheet and user documentation for details. For the latest product information, contact your local supplier or visit us online at www.interlogix.com.

Certification N4131

Complete additional sections according to the governing laws and standards for the intended market place.

FCC compliance This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

You are cautioned that any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

ACMA compliance Notice! This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

European Union directives 1999/5/EC (R&TTE directive): Hereby, UTC Building & Industrial Systems declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

2002/96/EC (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info.

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info.

Contact information For contact information, see www.interlogix.com/mobileview/.

Content

System Requirements 3

Camera Network Connections 4
Wiring over LAN 4
Detecting and Changing the IP Address 5

Accessing the Camera 6
Accessing by Web Browser 6

Live View 9
Live View Page 9
Starting Live View 10
Recording and Capturing Pictures Manually 10

Camera Configuration 11
Configuring Local Parameters 11
Configuring Time Settings 13
Configuring Network Settings 15
Configuring Video and Audio Settings 28
Configuring Image Parameters 31
Configuring and Handling Alarms 37
Handling Exception 42

Others 44
Managing User Accounts 44
Configuring RTSP Authentication 46
Anonymous Visit 47
IP Address Filter 48
Viewing Device Information 50
Maintenance 51
RS-232 Settings 53
Defog Settings (only available on MVC-9000) 54
IR Settings 54
Telnet Settings 54

System Requirements

Table 1: System Requirements

Operating System	Microsoft Windows XP SP1 and above /Vista/Win 7 32bits
CPU	Intel Premium IV 3.0 GHz or higher
RAM	1 GB or higher
Display	1024 x768 resolution or higher
Web Browser	Microsoft Explorer 6.0 and above, Mozilla Firefox 3.5 and above, Google Chrome 8 and above

Camera Network Connections

Wiring over LAN

The following figures show the two ways of cable connection of a network camera and a computer:

- To test the network camera, you can directly connect the network camera to a computer with a network cable as shown in Figure 1 below.
- Refer to Figure 2 below for connection of the network camera by LAN via a switch or a router.

Figure 1: Direct Connection

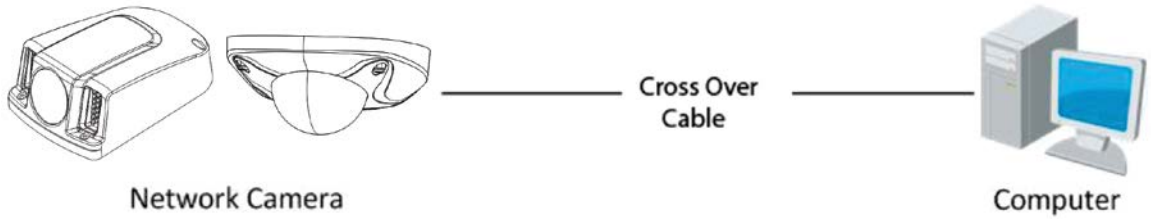
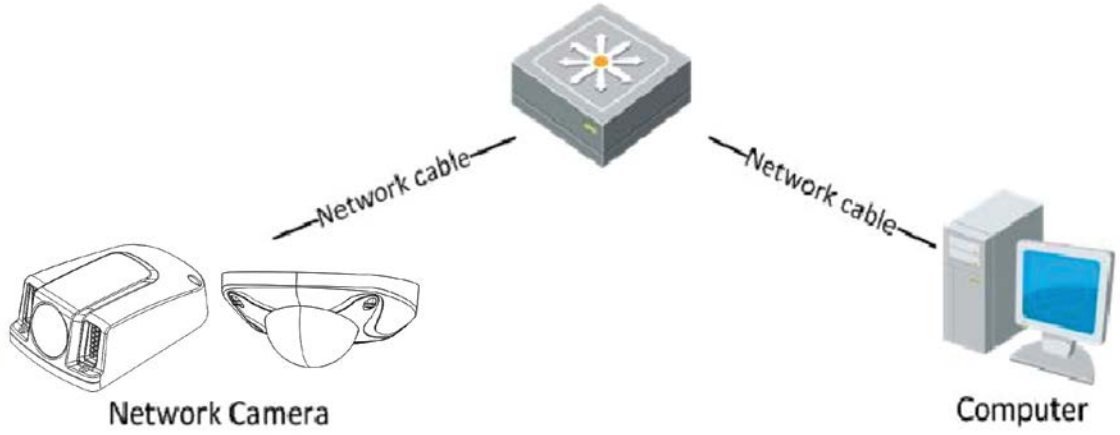


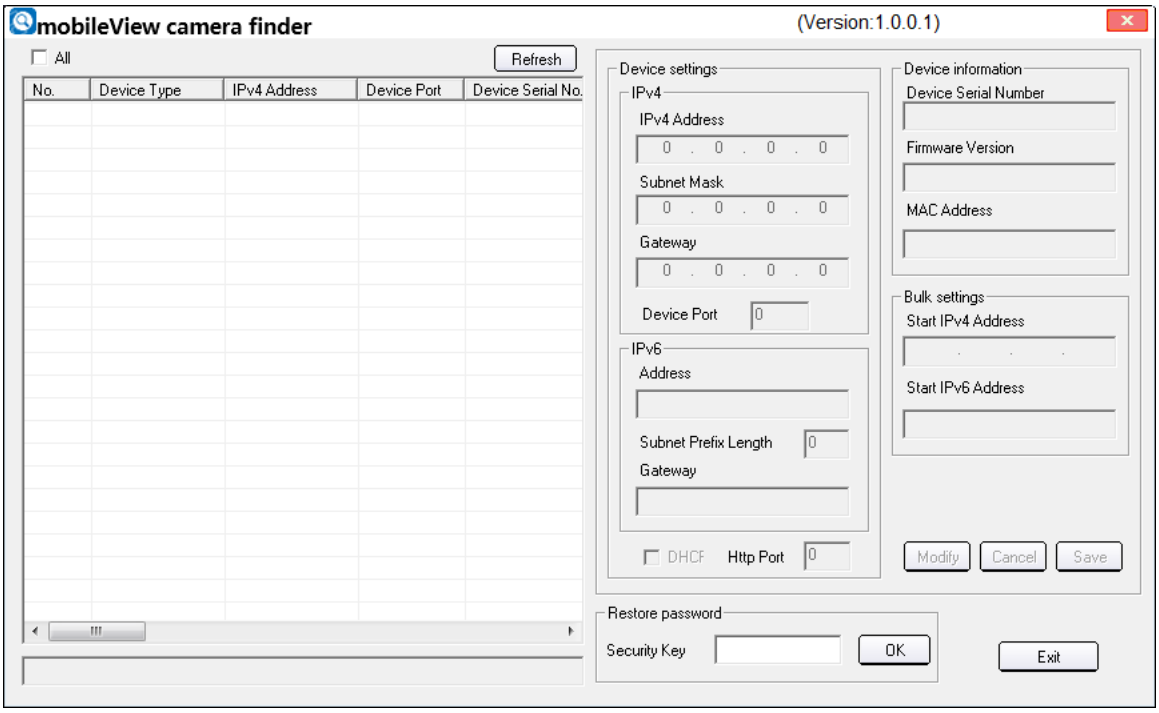
Figure 2: Connecting via a Switch or Router



Detecting and Changing the IP Address

You need the IP address of the camera to connect to the network camera using a computer. If you already know the IP address of the camera, skip to the next section, Accessing the Camera. The default IP address is 192.168.1.70, subnet is 255.255.255.0, and the port number is 8000. The default user name is admin, and password is 1234.

1. To get the IP address, you can install the Mobileview Camera Finder to list online devices.



2. To change the IP address and subnet mask as needed, input the new values in the appropriate fields, input the camera password, and click Save.

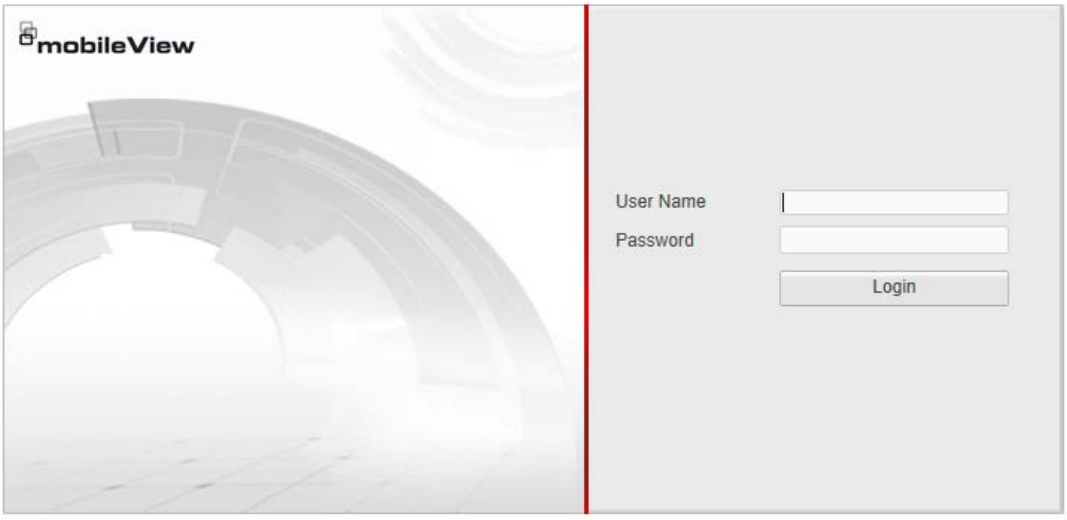
Accessing the Camera

Accessing by Web Browser

1. Open the web browser.
2. In the address field, input the IP address of the network camera, e.g., 192.168.1.70 and press the enter key to access the login interface.
3. Input the user name and password, and click ***Login***.

Note: The default user name is admin, and the password is 1234.

Figure 3: Login Interface



4. When prompted, please follow the installation prompts to install the plug-in.

Figure 4: Download and Install Plug-in

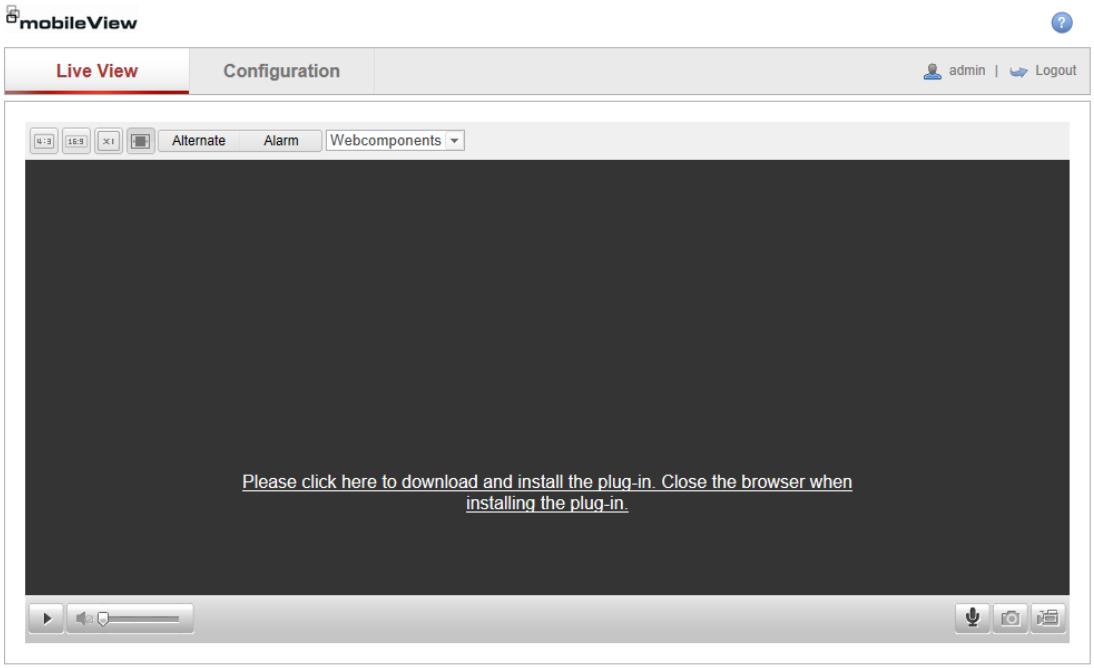


Figure 5: Install Plug-in (1)

Figure 6: install Plug-in (2)

Note: You must close the web browser to install the plug-in. Please reopen the web browser and log in again after the plug-in is installed.

Live View

Live View Page

The live video page allows you to view live video, capture images, and configure video parameters.

Once you are logged in to the camera, you can click Live View on the menu bar of the main page to enter the live view page.

Descriptions of the live view page:

Figure 7: Live View Page

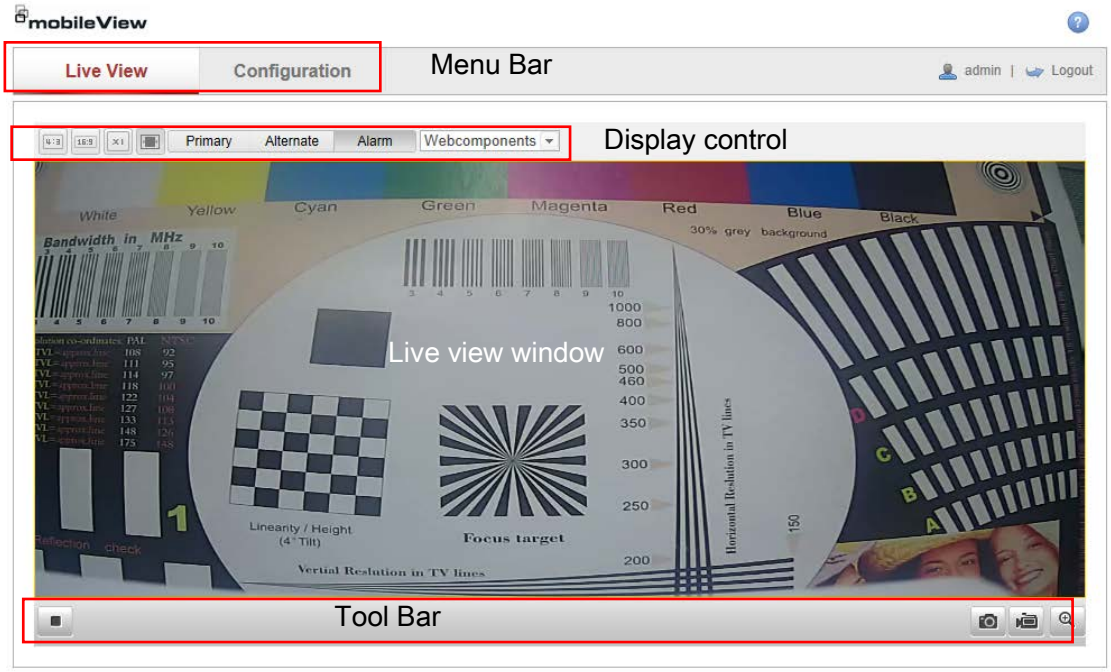


Table 2: Live View Page Options

Menu Bar	Click each tab to enter Live View and Configuration interface.
Display Control	Click each tab to adjust the layout and the stream type of the live view.
Live View Window	Display the live view.
Toolbar	Operations on the live view page, e.g., start/stop live view, capture, record, audio on/off, and digital zoom.

Starting Live View

In the live view window, click on the toolbar to start the live view of the camera.

Figure 8: Live View Toolbar

Table 3: Toolbar icon descriptions

Icon	Description
/	Start/Stop live view
	Manually capture the pictures displayed in live view and then save it as a JPEG file or BMP file.
/	Manually start/stop recording.
	Audio on and adjust volume /Mute. (Only available for MVC-9100)

Note: Before using audio, please set the **Stream Type** to **Video & Audio** (Only available for the 9100 Series Cameras).

Full-screen Mode

You can double-click on the live video to switch the current live view into full-screen or return to normal mode from the full-screen.

Recording and Capturing Pictures Manually

In the live view interface, click on the toolbar to capture the live pictures on your PC, or click to record the live video to your PC. The saving paths of the captured pictures and clips can be set on the **Configuration>Local Configuration** page.

Note: The captured image will be saved as JPEG or BMP file in your computer.

Camera Configuration

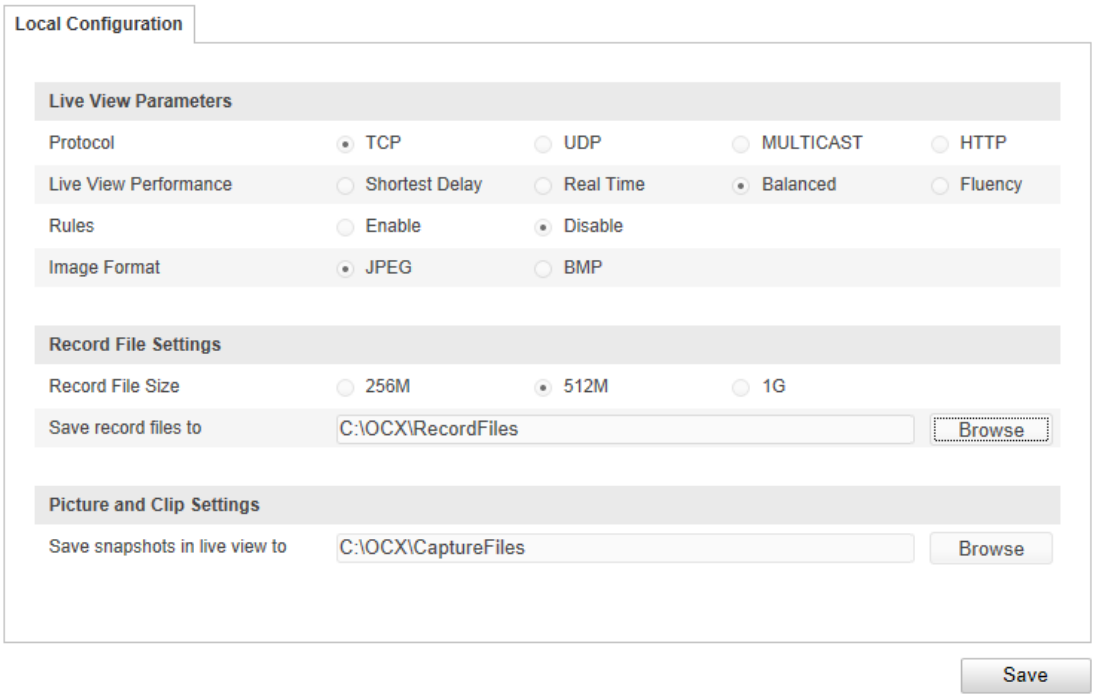
Configuring Local Parameters

Note: Local configuration refers to the parameters for live view, recorded video files, and captured pictures. The recorded files and captured pictures are the ones you saved using the web browser and thus the files were saved to the defined locations on the PC running the browser.

1. Enter the Local Configuration interface:

   Configuration > Local Configuration

Figure 9: Local Configuration Interface



2. Configure the following settings:

Live View Parameters	**Protocol Type:** TCP, UDP, MULTICAST and HTTP are selectable. **TCP:** Ensures complete delivery of streaming data and better video quality, yet the real-time transmission will be affected. **UDP:** Provides real-time audio and video streams. **HTTP:** Allows the same quality as of TCP without setting specific ports for streaming under some network environments. **MULTICAST:** It's recommended to select MCAST type when using the Multicast function. For detailed information about Multicast, refer to Configuring TCP/IP Settings *on page 15.* **Live View Performance:** Set the live view performance to Shortest Delay, Real Time, Balanced or Fluency.
Record File Settings	**Record File Size:** Select the packed size of the manually recorded and downloaded video files to 256M, 512M or 1G. After the selection, the maximum record file size is the value you selected. **Save record files to:** Set the folder location for the manually recorded video files. **Save snapshots in live view to:** Set the folder location of the pictures captured manually in live view mode.

Note: You can click Browse to change the directory for saving the video files and pictures.

3. Click **Save** to save the settings.

Configuring Time Settings

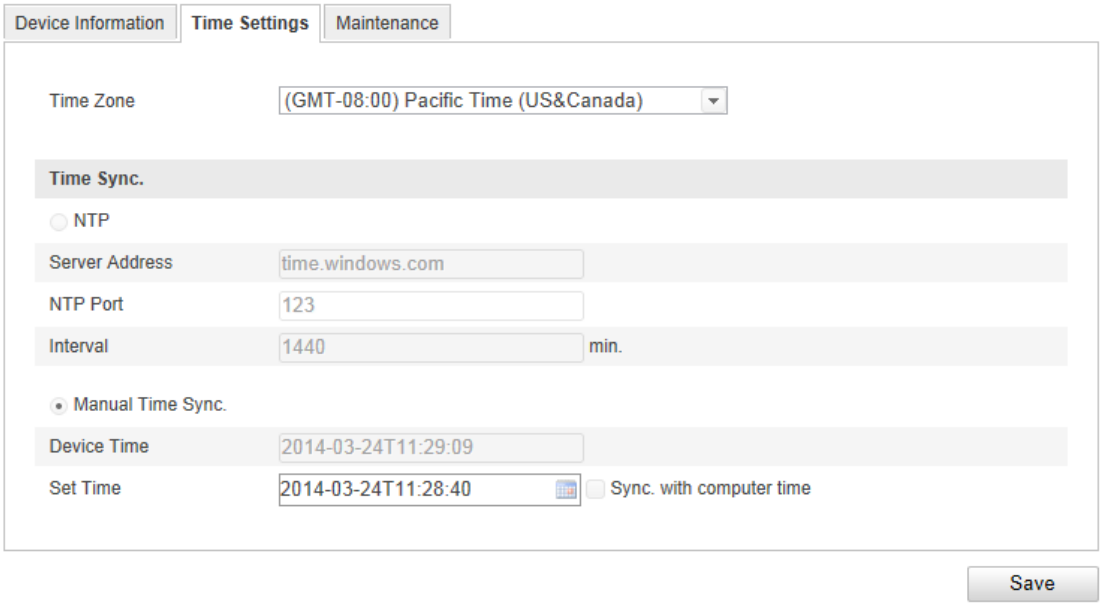
You can follow the instructions in this section to configure the time synchronization and DST settings.

1. Enter the Time Settings interface:

   Configuration> Basic Configuration > System > Time Settings

   Or **Configuration > Advanced Configuration > System > Time Settings**

Figure 10: Time Settings



- Select the Time Zone.

  Select the Time Zone where the camera is located from the drop-down menu.

- Synchronizing Time by NTP Server.

  Check the checkbox to enable the **NTP** function.

  Configure the following settings:

  Server Address: IP address of NTP server.

  NTP Port: Port of NTP server.

  Interval: The time interval between the two synchronizing actions with NTP server.

Figure 11: Time Sync by NTP Server

Note: If the camera is connected to a public network, you should use a NTP server that has a time synchronization function, such as the server at the National Time Center (IP Address: 210.72.145.44). If the camera is set in a customized network, NTP software can be used to establish a NTP server for time synchronization.

- Synchronizing Time Synchronization Manually

  Enable the **Manual Time Sync** function and then click to set the system time from the pop-up calendar.

Note: You can also check the **Sync with computer time** checkbox to synchronize the time of the camera with that of your computer.

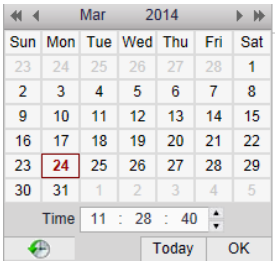
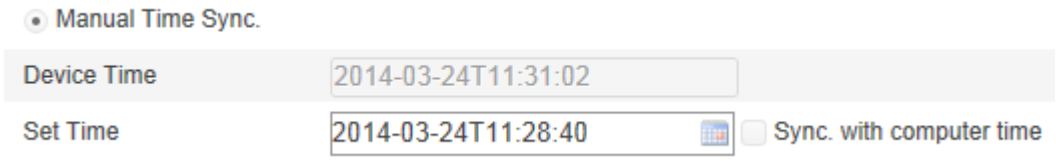
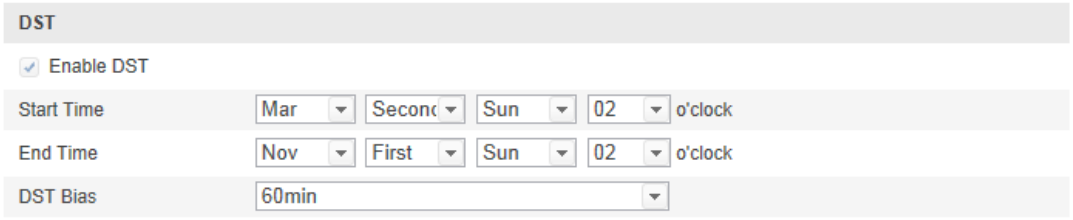


Figure 12: Manual Time Sync



- Click DST tab to enable the DST function and set the date of the DST period.

Figure 13: DST Settings



2. Click **Save** to save the settings.

Configuring Network Settings

Configuring TCP/IP Settings

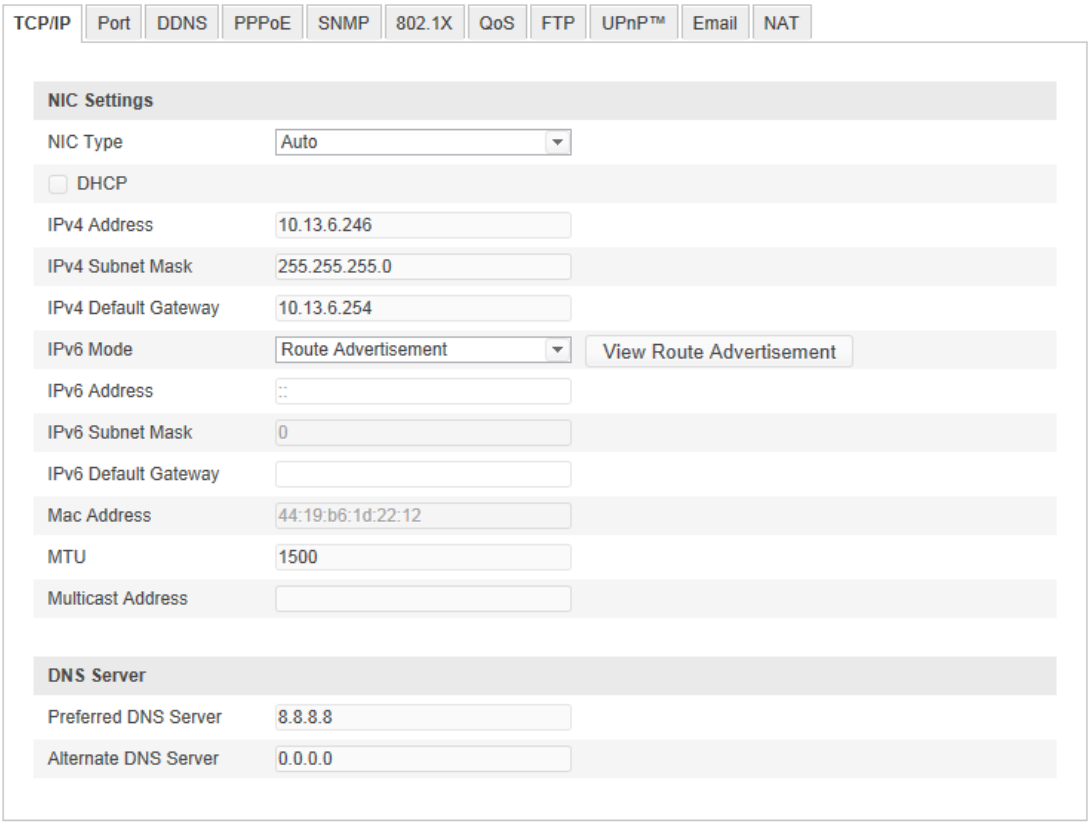
TCP/IP settings must be properly configured before you operate the camera over a network. The camera supports both IPv4 and IPv6. Both versions may be configured simultaneously without conflict. At least one IP version should be configured.

1. Enter TCP/IP Settings interface:

   Configuration > Basic Configuration > Network> TCP/IP

   Or **Configuration > Advanced Configuration> Network > TCP/IP**

Figure 14: TCP/IP Settings



2. Configure the basic network settings, including the NIC Type, IPv4 or IPv6 Address, IPv4 or IPv6 Subnet Mask, IPv4 or IPv6 Default Gateway, MTU settings and Multicast Address.

   - The valid value range of MTU is 500 ~ 1500.
   - The Multicast sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Before utilizing this function, you must enable the Multicast function of your router.

3. Click **Save** to save the above settings.

Note: A reboot is required for the settings to take effect.

Configuring Port Settings

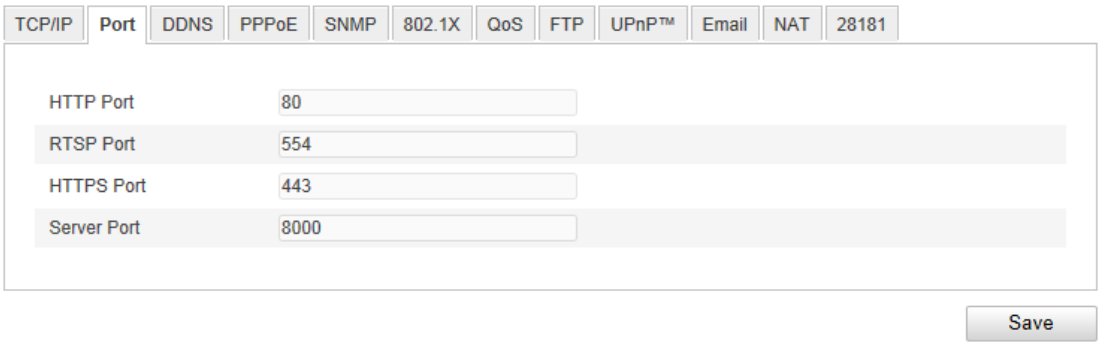
You can set the ports of the camera, e.g. HTTP port, RTSP port and HTTPS port.

1. Enter the Port Settings interface:

Configuration > Basic Configuration > Network> Port

Or **Configuration > Advanced Configuration> Network > Port**

Figure 15: Port Settings



2. Set the HTTP port, RTSP port and HTTPS port of the camera.

HTTP Port	The default port number is 80. If you change it, it is recommended to use a port within the range 1024 to 65535.
RTSP Port	The default port number is 554.
HTTPS Port	The default port number is 443. If you change it, it is recommended to use a port within the range 1024 to 65535.
Server Port	The default server port number is 8000.

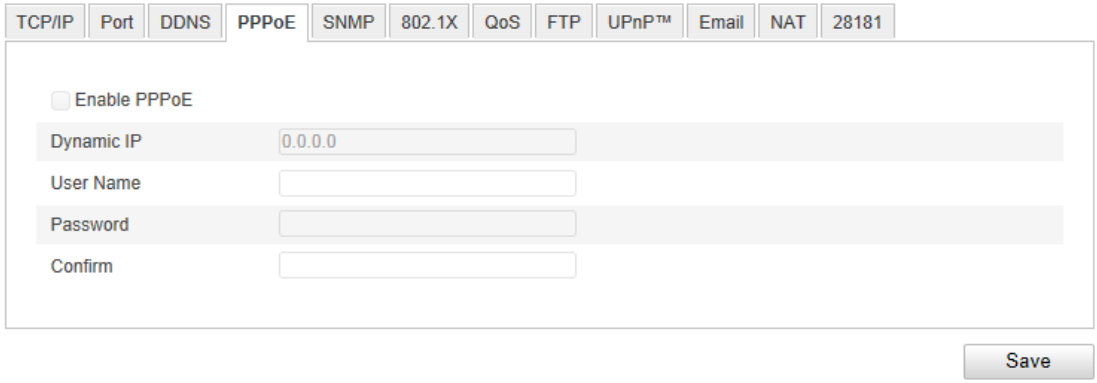
3. Click **Save** to save the settings.
4. A reboot is required for the settings to take effect.

Configuring PPPoE Settings

1. Enter the PPPoE Settings interface:

   Configuration> Advanced Configuration > Network > PPPoE

Figure 16: PPPoE Settings



2. Check the **Enable PPPoE** checkbox to enable this feature.
3. Enter **User Name**, **Password**, and **Confirm** password for PPPoE access.

   The User Name and Password should be assigned by your ISP.

4. Click **Save** to save and exit the interface.
5. A reboot is required for the settings to take effect.

Configuring DDNS Settings

If your camera is set to use PPPoE as its default network connection, you can use the Dynamic DNS (DDNS) for network access.

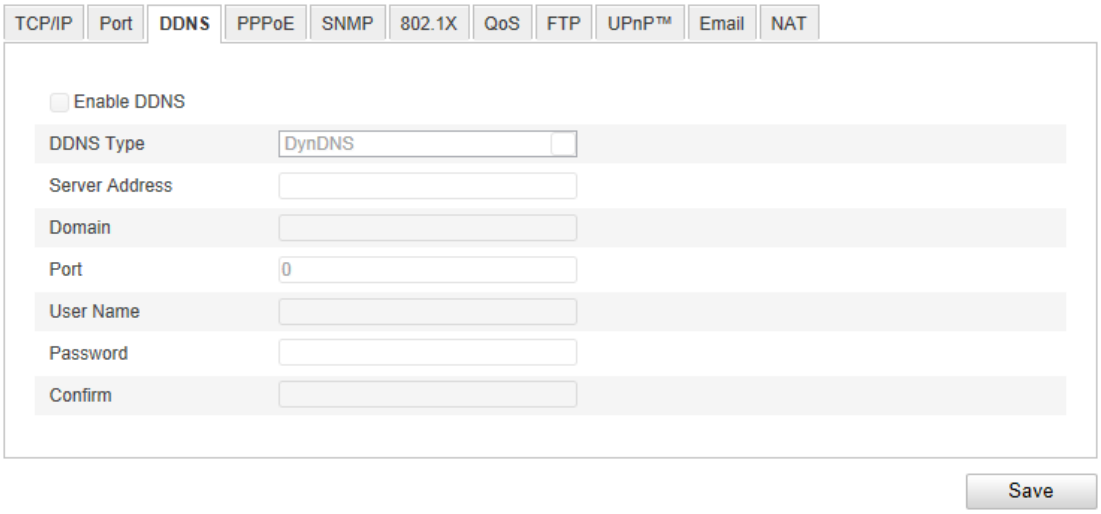
Before you start:

Registration on the DDNS server is required before configuring the DDNS settings of the camera.

1. Enter the DDNS Settings interface:

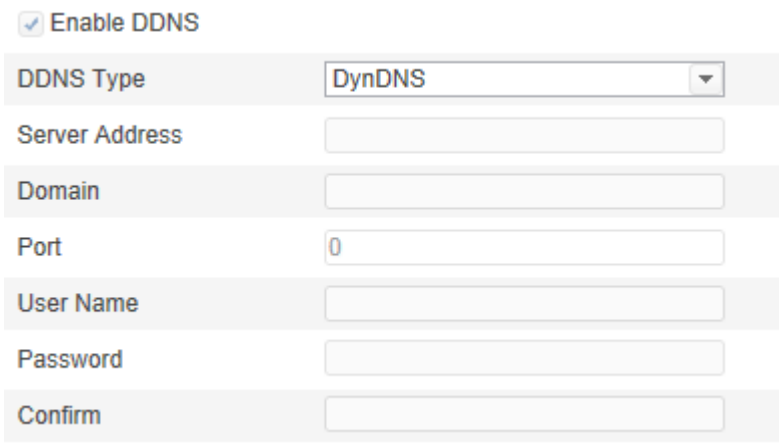
   Configuration > Advanced Configuration> Network > DDNS

Figure 17: DDNS Settings



2. Check the **Enable DDNS** checkbox to enable this feature.
3. Select **DDNS Type**. Three DDNS types are selectable: DynDNS, IPServer and No-IP. When selecting DynDNS follow these steps:
    - Enter **Server Address** of DynDNS (e.g. members.dyndns.org).
    - In the **Domain** text field, enter the domain name obtained from the DynDNS website.
    - Enter the **Port** of DynDNS server.
    - Enter the **User Name** and **Password** registered on the DynDNS website.
    - Click **Save** to save the settings.

Figure 18: DynDNS Settings



When selecting IP Server follow the steps below:

- Enter the Server Address of the IP Server.
- Click **Save** to save the settings.

Note: For the IP Server, you must apply a static IP, subnet mask, gateway and preferred DNS from the ISP. The **Server Address** should be entered with the static IP address of the computer that runs the IP Server software.

Figure 19: IP Server Settings

For the US and Canada area, you can enter 173.200.91.74 as the server address.

When selecting NO-IP follow the steps below:

- Choose the DDNS Type as NO-IP.

Figure 20: Login Interface

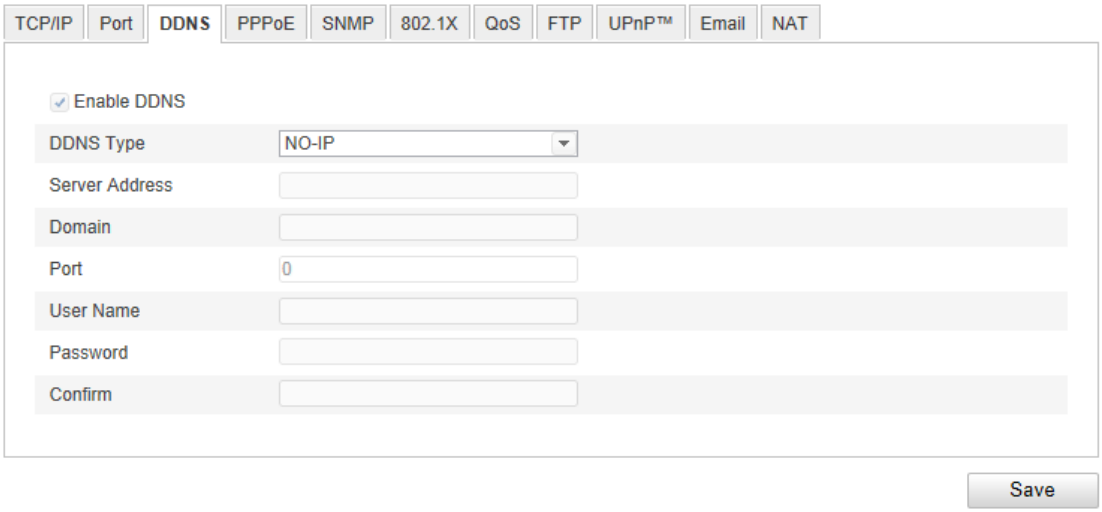


Figure 1-1 NO-IP Settings

- Enter the Server Address.
- Enter the Domain name of the camera, user name and password.
- Click **Save** to save the new settings.
- A reboot is required for the settings to take effect.

Configuring SNMP Settings

You can set the SNMP function to get camera status, parameters, and alarm-related information, and manage the camera remotely when it is connected to the network.

Before you start:

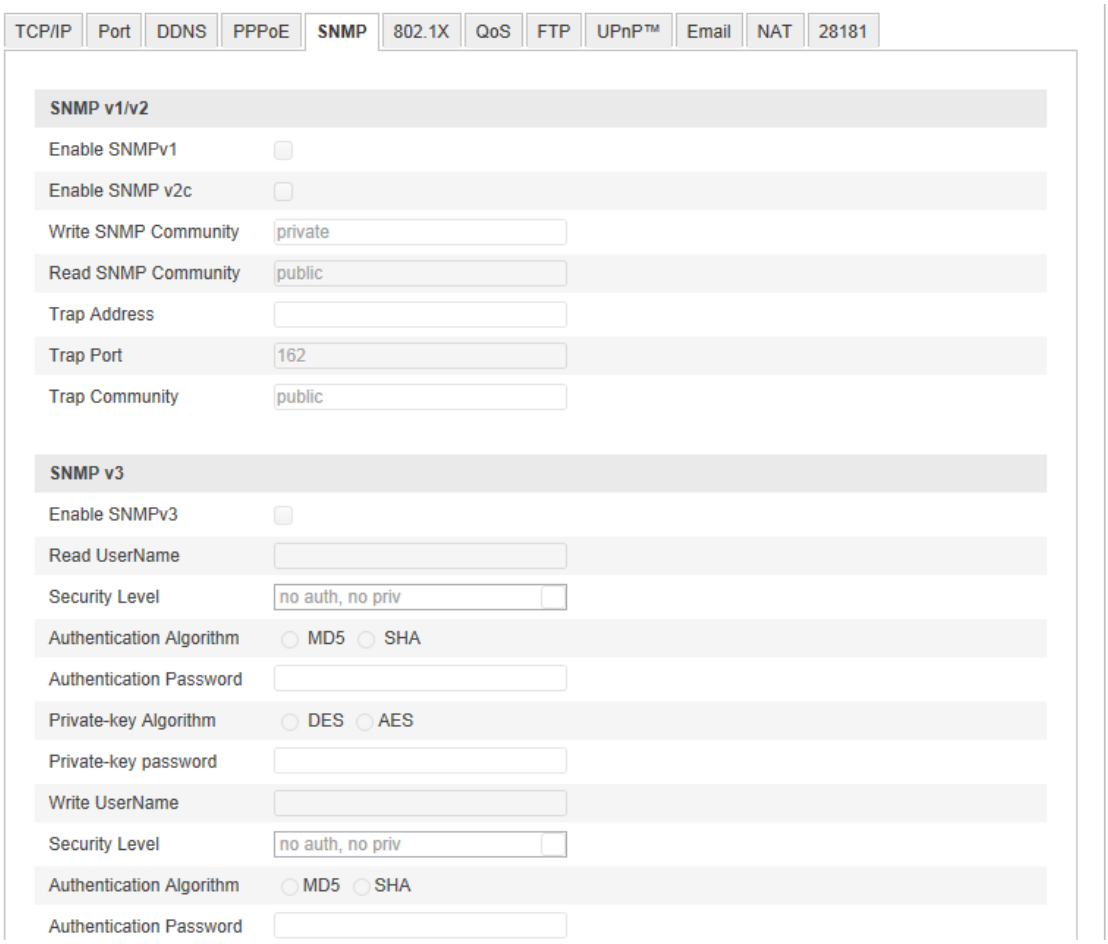
Before setting the SNMP, please download SNMP software and verify you receive the camera information via SNMP port. By setting the Trap Address, the camera can send the alarm event and exception messages to the surveillance center.

The SNMP version you select should be the same as that of the SNMP software. And you also need to use the specific version according to the security level you require. SNMP v1 provides no security, SNMP v2 requires password for access, and SNMP v3 provides encryption. If you use v3, HTTPS protocol must be enabled.

1. Enter the SNMP Settings interface:

   Configuration > Advanced Configuration > Network> SNMP

Figure 21: SNMP Settings



2. Check the corresponding version checkbox (Enable SNMPv1 , Enable SNMP v2c , Enable SNMPv3) to enable the feature.
3. Configure the SNMP settings. The settings of the SNMP software should be the same as the settings you configure here.
4. Click **Save** to save and finish the settings.
5. A reboot is required for the settings to take effect.

Configuring 802.1X Settings

The IEEE 802.1X standard is supported by the cameras and, when the feature is enabled, the camera data is secured and user authentication is needed when connecting the camera to the network protected by the IEEE 802.1X.

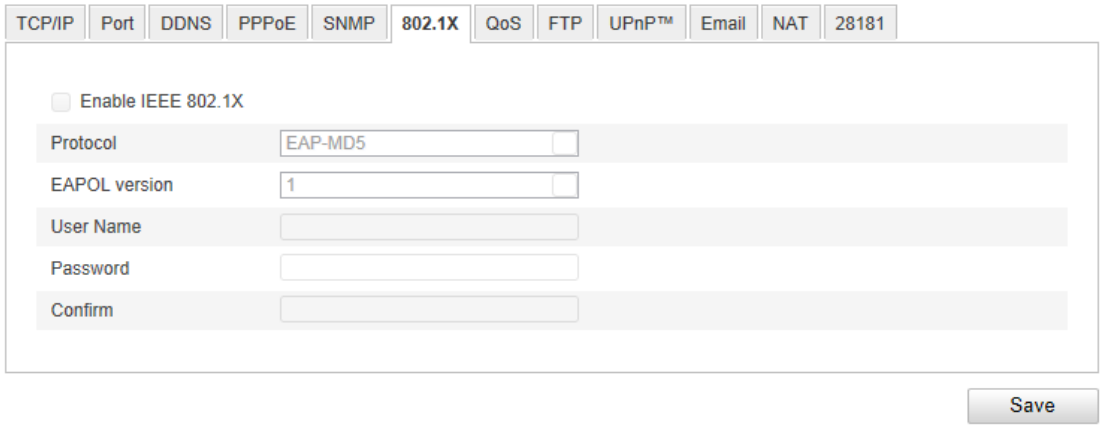
Before you start:

The authentication server must be configured. Please apply and register a user name and password for 802.1X in the server.

1. Enter the 802.1X Settings interface:

   Configuration > Advanced Configuration > Network> 802.1X

Figure 22: 802.1X Settings



2. Check the **Enable IEEE 802.1X** checkbox to enable the feature.
3. Configure the 802.1X settings, including EAPOL version, user name and password. The EAPOL version must be identical with that of the router or the switch.
4. Enter the user name and password to access the server.
5. Click Save to finish the settings.
6. A reboot is required for the settings to take effect.

Configuring QoS Settings

QoS (Quality of Service) can help solve network delays and congestion by configuring the priority of data traffic.

1. Enter the QoS Settings interface:

   Configuration >Advanced Configuration> Network > QoS

Figure 23: QoS Settings

2. Configure the QoS settings, including video / audio DSCP, event / alarm DSCP, and Management DSCP.

   The valid value range of the DSCP is 0-63. The bigger the DSCP value, the higher the priority. SCP refers to the Differentiated Service Code Point; and the DSCP value is used in the IP header to indicate the priority of the data.

3. Click **Save** to save the settings.
4. A reboot is required for the settings to take effect.

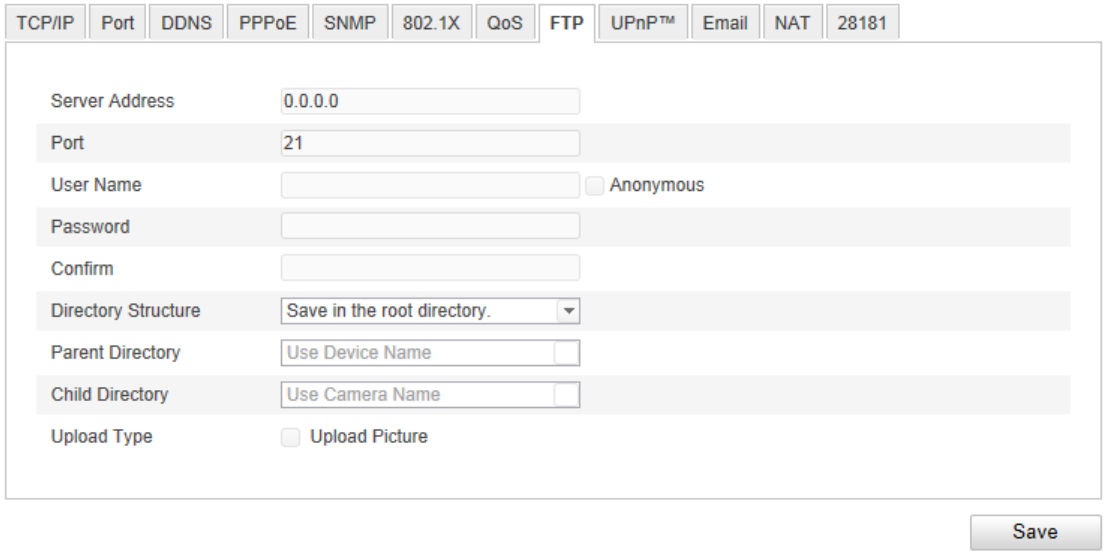
Configuring FTP Settings

You can configure the FTP server information to enable the uploading of the captured pictures to the FTP server. The captured pictures can be triggered by events or a timing snapshot task.

1. Enter the FTP Settings interface:

   Configuration >Advanced Configuration> Network > FTP

Figure 24: FTP Settings



2. Configure the FTP settings; the user name and password are required for login to the FTP server.

   Directory: In the **Directory Structure** field, you can select the root directory, parent directory, and child directory. When the parent directory is selected, you have the option to use the Device Name, Device Number or Device IP for the name of the directory; and when the Child Directory is selected, you can use the Camera Name or Camera No. as the name of the directory.

Upload type: To enable uploading the captured picture to the FTP server.

Anonymous Access to the FTP Server (in which case the user name and password won't be requested.)**:** Check the Anonymous checkbox to enable the anonymous access to the FTP server.

Note: The anonymous access function must be supported by the FTP server.

3. Click **Save** to save the settings.

Note: If you want to upload the captured pictures to FTP server, you must enable the continuous snapshot or event-triggered snapshot on the **Snapshot** page.

Configuring UPnP™ Settings

Universal Plug and Play (UPnP™) is a networking architecture that provides compatibility among networking equipment, software, and other hardware devices. The UPnP protocol allows devices to connect seamlessly and simplifies the implementation of networks at home and in corporate environments.

With the function enabled, you don't need to configure the port mapping for each port, and the camera is connected to the Wide Area Network via the router.

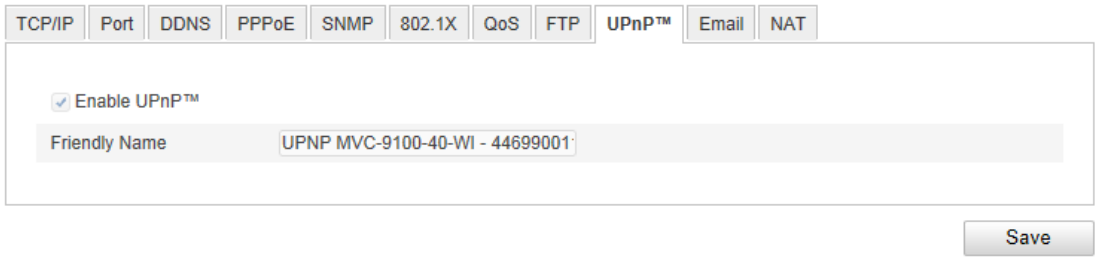
1. Enter the UPnP™ settings interface.

   Configuration >Advanced Configuration> Network > UPnP

2. Check the checkbox to enable the UPnP™ function.

   The name of the device, when detected online, can be edited.

Figure 25: Configure UPnP Settings



Configuring Email Settings

The system can be configured to send an Email notification to all designated receivers if an alarm event is detected, e.g., motion detection event, video loss, video tampering, etc.

Before you start:

Please configure the DNS Server settings under **Basic Configuration >**

Network> TCP/IP or **Advanced Configuration > Network > TCP/IP** before using the Email function.

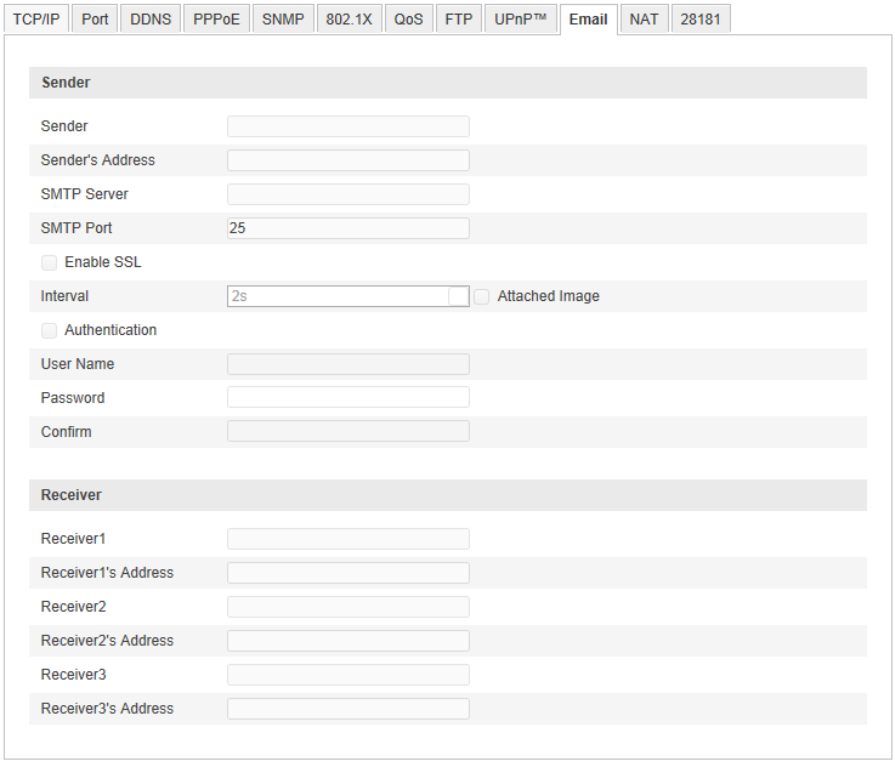
1. Enter the TCP/IP Settings (**Configuration> Basic Configuration > Network > TCP/IP** or **Configuration > Advanced Configuration> Network > TCP/IP)** to set the IPv4 Address, IPv4 Subnet Mask, IPv4 Default Gateway, and the Preferred DNS Server.

Note: Please refer to ***Configuring TCP/IP Settings*** for details.

2. Enter the Email Settings interface:

Configuration > Advanced Configuration > Network > Email

Figure 26: Email Settings



3. Configure the following settings:

Sender	The name of the email sender.
Sender's Address	The email address of the sender.

SMTP Server	The SMTP Server IP address or host name (e.g., smtp.263xmail.com).
SMTP Port	The SMTP port. The default TCP/IP port for SMTP is 25 (not secured). And the SSL SMTP port is 465.
Enable SSL	Check the checkbox to enable SSL if it is required by the SMTP server.
Attached Image	Check the checkbox of Attached Image if you want to send emails with attached alarm images.
Interval	The interval refers to the time between two actions of sending attached pictures.
Authentication	If your email server requires authentication, check this checkbox to use authentication to log in to this server and enter the login user Name and password.
Choose Receiver	Select the receiver to which the email is sent. Up to 2 receivers can be configured.
Receiver	The name of the user to be notified.
Receiver's Address	The email address of user to be notified.

4. Click **Save** to save the settings.

Configuring NAT (Network Address Translation) Settings

1. Enter the NAT settings interface.

   Configuration >Advanced Configuration> Network > NAT

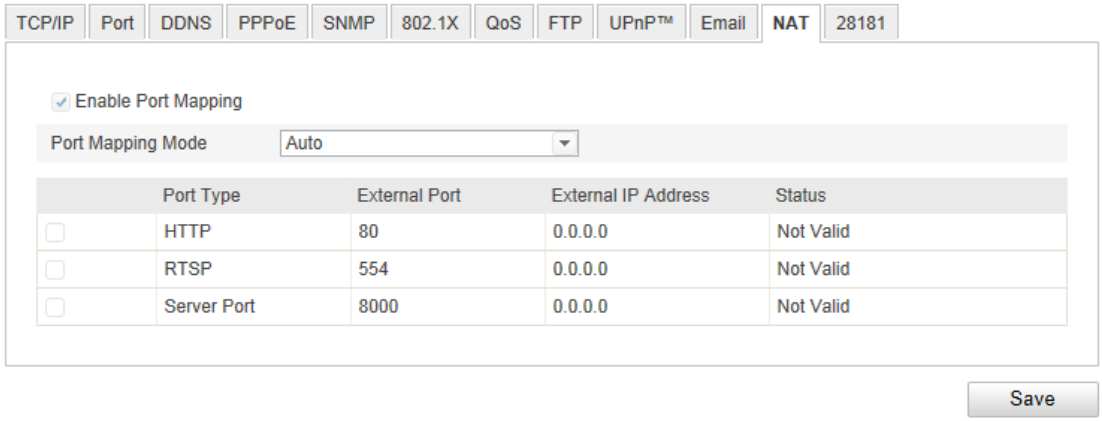
2. Choose the port mapping mode.

   To port mapping with the default port number, you can choose **Port Mapping Mode** as **Auto**.

   To port mapping with the customized port numbers, you can choose **Port Mapping Mode** as **Manual**.

   And for manual port mapping, you can customize the value of the port number by yourself.

Figure 27: Configure NAT Settings



3. Click **Save** to save the settings.

Configuring Video and Audio Settings

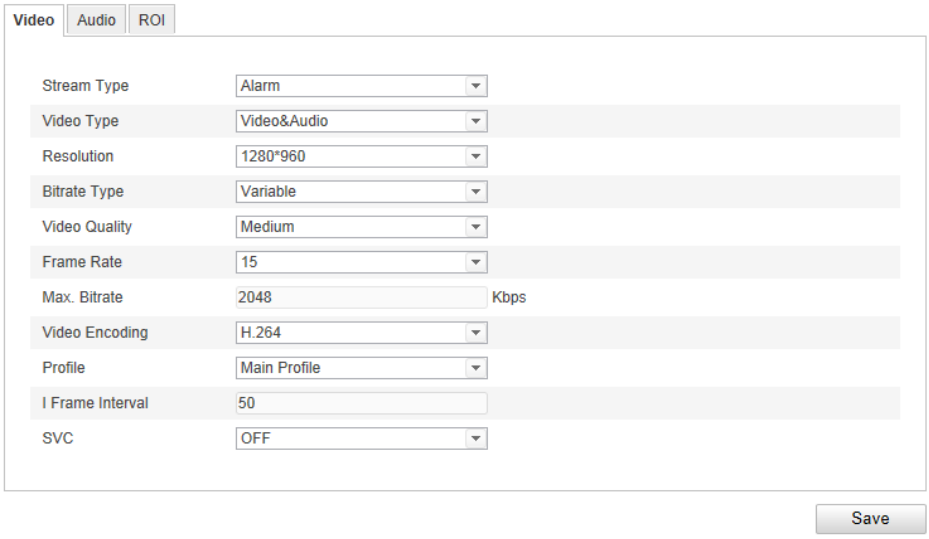
Configuring Video Settings

1. Enter the Video Settings interface:

   Configuration> Basic Configuration > Video / Audio > Video

   Or **Configuration > Advanced Configuration > Video / Audio > Video**

Figure 28: Confgure Video Settings



2. Select the **Stream Type** of the camera to Alarm stream, Primary stream or Alternate stream.

   The Alarm stream is usually for live viewing and recording in response to

alarm events, the Primary stream is for normal recording, and the Alternate stream can be used for live viewing over cellular or for low-bandwidth archival.

3. You can customize the following parameters for the selected main stream or sub-stream:

Video Type	Select the stream type to video stream, or video & audio composite stream. The audio signal will be recorded only when the **Video Type** is **Video & Audio**. (Audio only available on MVC-9100)
Resolution	Select the resolution of the video output.
Bitrate Type	Select the bitrate type to constant or variable.
Video Quality	When bitrate type is selected as **Variable**, 6 levels of video quality are selectable.
Frame Rate	Set the frame rate to 1/16~30 fps. The frame rate is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.
Max. Bitrate	Set the max. bitrate to 64-6144 Kbps. The higher value corresponds to better video quality, but higher bandwidth and storage space is required.
Video Encoding	If the **Stream Type** is set to Alarm or Primary stream, H.264 is selectable; if the stream type is set to Alternate stream, H.264, and MJPEG are selectable. The supported video encoding may differ according to the platform.
Profile	Select the profile from the drop-down menu.
I Frame Interval	Set the I-Frame interval to 1~400.
SVC	Scalable Video Coding is an extension of the H.264/AVC standard. Set it OFF or ON according to your actual needs.

4. Click **Save** to save the settings.

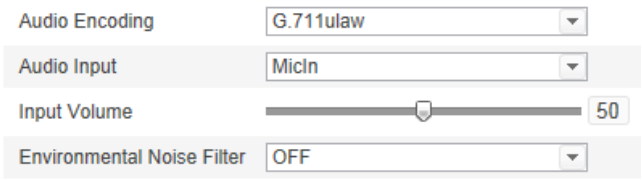
Configuring Audio Settings (Only available on MVC-9100)

1. Enter the Audio Settings interface

   Configuration> Basic Configuration > Video / Audio > Audio

   Or **Configuration > Advanced Configuration > Video / Audio > Audio**

Figure 29: Audio Settings



2. Configure the following settings.

   Audio Encoding: G.711 ulaw, G.711alaw, G.726, and MP2L2 are selectable. And 32kbps, 64kbps, and 128kbps are supported if MP2L2 is selected.

   Audio Input: Only MicIn is available for the microphone.

3. Click **Save** to save the settings.

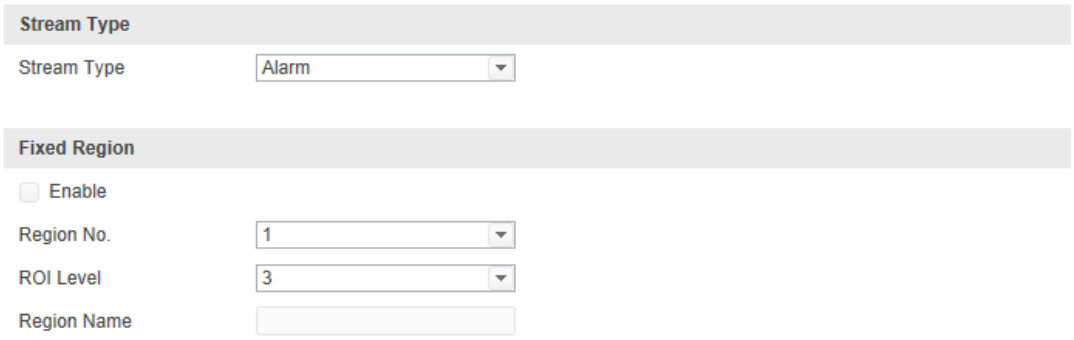
Configuring ROI Settings

ROI stands for the region of interest. The ROI encoding enables you to discriminate the ROI and background information in compression, that is to say, the technology assigns more encoding resource to the region of interest to increase the quality of the ROI whereas the background information is less focused.

1. Enter the ROI settings interface

   Configuration > Advanced Configuration> Video / Audio >ROI

Figure 30: Login Interface



2. Draw the region of interest on the image. Four regions can be drawn.
3. Choose the stream type to set the ROI encoding.
4. Configuring ROI.

   There are two options for ROI encoding, the fixed region encoding and the dynamic tracking.

   The fixed region encoding is the ROI encoding for the manually configured area. And you can choose the Image Quality Enhancing level for ROI encoding, and you can also name the ROI area.

4. Click **Save** to save the settings.

Configuring Image Parameters

Configuring Display Settings

You can set the image quality of the camera, including brightness, contrast, saturation, hue, sharpness, etc.

The Display parameters vary depending on the camera model.

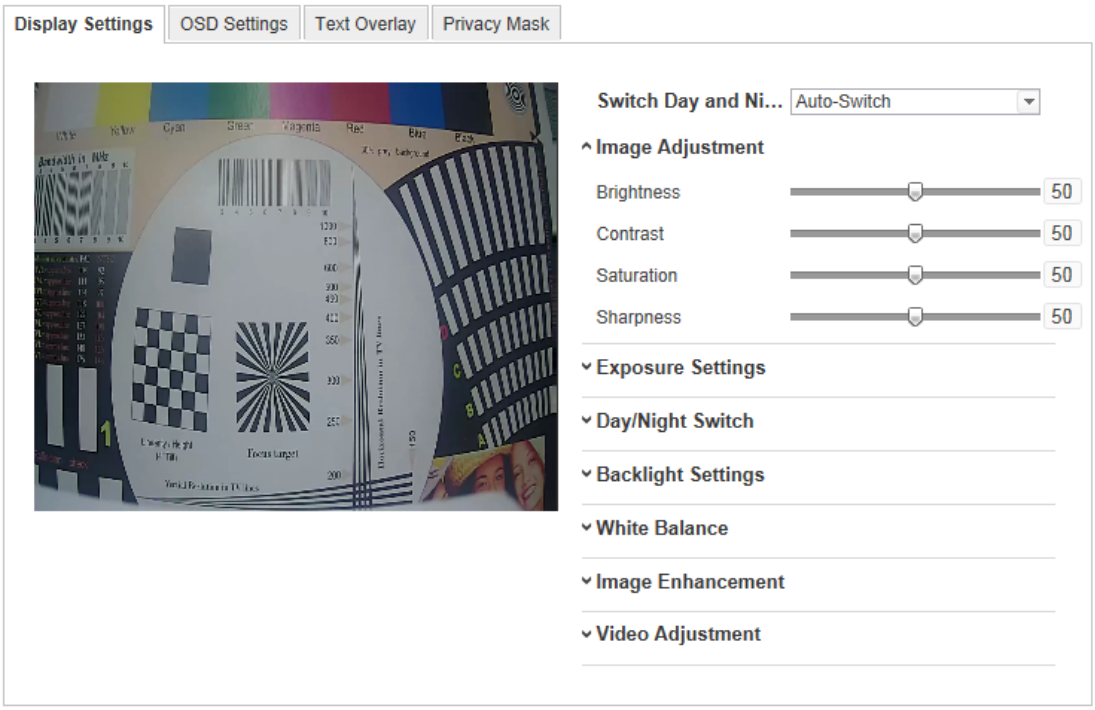
1. Enter the Display Settings interface:

Configuration> Basic Configuration> Image> Display Settings

Or Configuration > Advanced Configuration> Image> Display Settings

2. Set the image parameters of the camera

Figure 31: Display Settings



Descriptions of parameter configuration

Image Adjustment

Brightness describes the brightness of the image, which ranges from 1~100, and the default value is 50.

Contrast describes the contrast of the image, which ranges from 1~100, and the default value is 50.

Saturation describes the colorfulness of the image color, which ranges from 1~100, and the default value is 50.

Sharpness describes the edge contrast of the image, which ranges from 1~100, and the default value is 50.

Exposure Settings

Exposure Time: Value ranges from 1/3 to 1/100,000s. Adjust it according to the lighting condition.

Gain: Select the value to adjust the image brightness.

Iris Mode: Only Manual is selectable.

Day/Night Switch

Select the day/night switch mode, and configure the smart IR settings from this option.
Day, night, auto, schedule, and triggered by alarm input are selectable for day/night switch.

Day: the camera stays at day mode.

Night: the camera stays at night mode.

Auto: the camera automatically switches between day mode and night mode according to ambient illumination. The sensitivity ranges from 0~7; the higher the value, the easier the mode switches. The filtering time refers to the interval time between the day/night switch. You can set it from 5s to 120s.

Schedule: Set the start time and the end time to define the duration for day/night mode.

Sensitivity: If you choose auto day/night switch, you can choose the sensitivity of the switch as high, normal and low.

Smart IR gives user an option to adjust the IR LED intensity. Auto Mode reduces likelihood of over-exposure due to unnecessarily bright IR light.

Backlight Settings

WDR:

Wide dynamic range can be used when there is a high contrast of the bright area and the dark area of the scene.

BLC Area:

BLC area is the area sense the light intensity; Close, Up, Down, Left, Right and Center are selectable.

White Balance

The below figure shows the white balance type selectable. You can choose it according to the real condition. For example, if in the surveillance scene, there is a fluorescent lamp, you can choose the white balance type as the Fluorescent Lamp.

Figure 32: White Balance

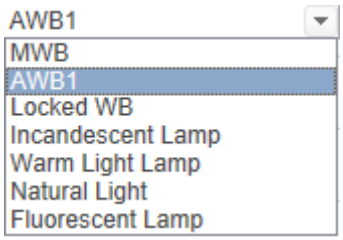


Image Enhancement

Digital Noise Reduction:

Off, Normal Mode and Expert Mode are selectable.

Noise Reduction Level:

For adjusting the noise reduction level and only valid when the DNR function is enabled.

Video Adjustment

Video Standard:

50 Hz and 60 Hz are selectable. Choose according to the different video standards; normally 50Hz for PAL standard and 60Hz for NTSC standard.

Mirror：

The mirror function enables you to flip the image horizontally and vertically.

Rotate mode:

To make a complete use of the 16:9 aspect ratio, you can enable the rotate mode when you use the camera in a narrow view scene.

When installing, turn the camera to 90 degrees or rotate the 3-axis lens to 90 degrees, and set the rotate mode as on, you will get a normal view of the scene with 9:16 aspect ratio to ignore the needless information such as the wall, and get more meaningful information of the scene.

Capture Mode:

This is the selectable video input mode to meet the different demands of field of view and resolution.

Local Output:

With this option, you can enable or disable the BNC analog output.

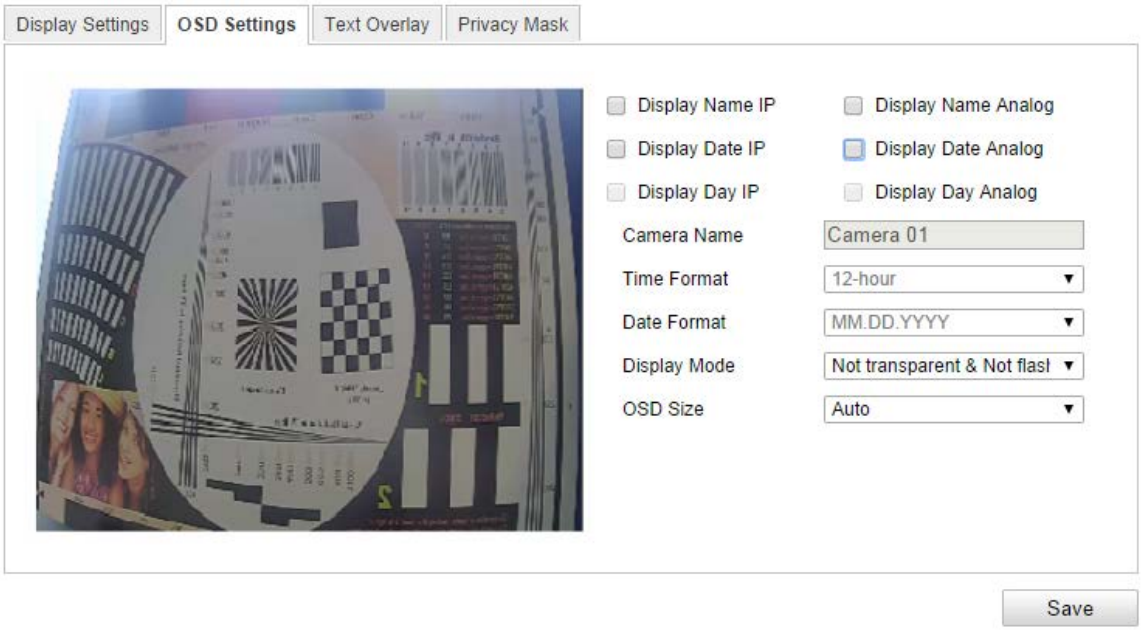
Configuring OSD Settings

You can customize the camera name and time on the screen.

1. Enter the OSD Settings interface:

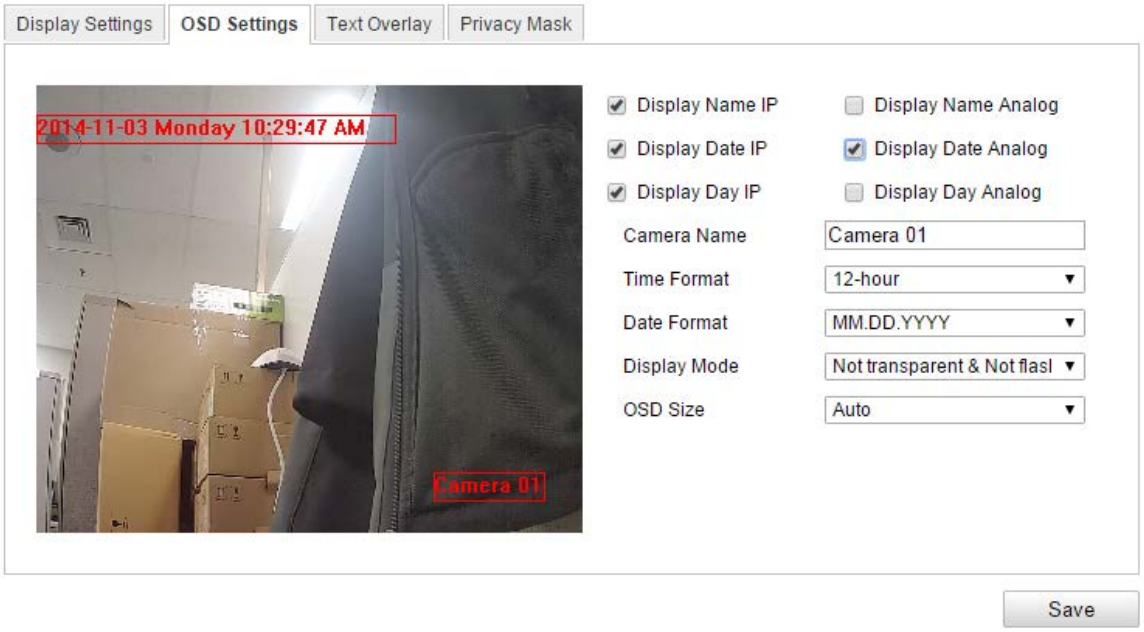
Configuration> Advanced Configuration > Image > OSD Settings

Figure 33: OSD Settings



2. Check the corresponding checkbox to select the display of camera name, date or day if required. These can be selectively displayed on the IP Streams, the Analog output, or both.
3. Edit the camera name in the text field of **Camera Name**.
4. Select from the drop-down list to set the time format, date format, display mode and the OSD font size.
5. You can use the mouse to click and drag the text frame Camera 01 in the live view window to adjust the OSD position.

Figure 34: Adjust OSD Location



6. Click **Save** to activate above settings.

Configuring Text Overlay Settings

You can customize the text overlay.

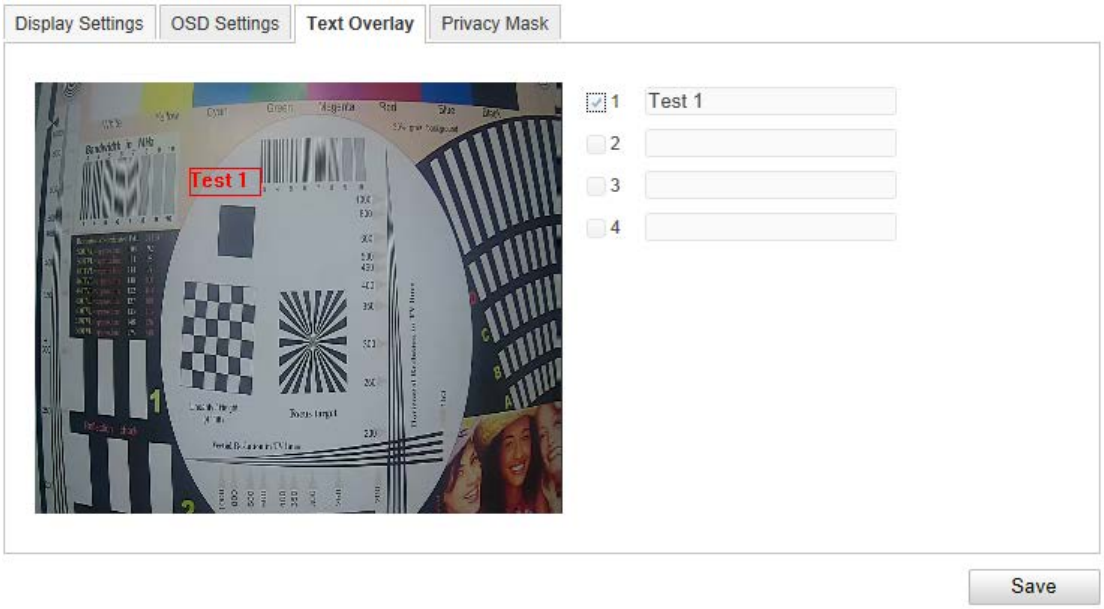
1. Enter the Text Overlay Settings interface:

   Configuration> Advanced Configuration > Image > Text Overlay

2. Check the checkbox in front of textbox to enable the on-screen display.
3. Input the characters in the textbox.
4. Use the mouse to click and drag the red text frame Test 1 in the live view window to adjust the text overlay position.
5. Click **Save**.

Note: Up to 4 text overlays are configurable.

Figure 35: Text Overlay Settings



Configuring Privacy Mask

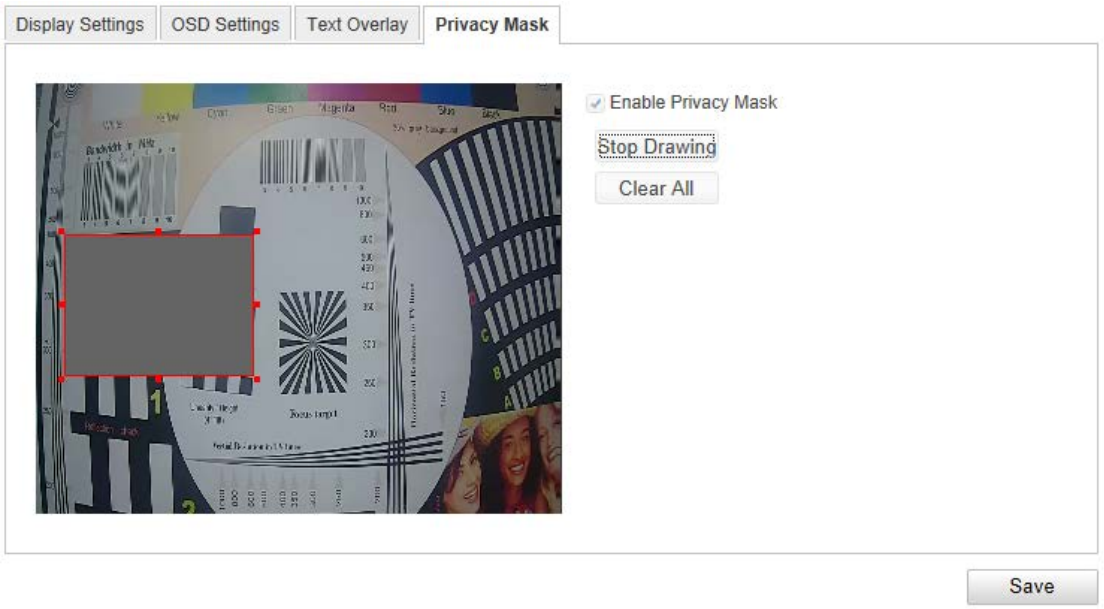
Privacy mask enables you to cover certain areas on the live video to prevent certain spots in the surveillance area from being live viewed and recorded.

1. Enter the Privacy Mask Settings interface:

Configuration> Advanced Configuration> Image > Privacy Mask

2. Check the checkbox of **Enable Privacy Mask** to enable this function.
3. Click Draw Area.

Figure 36: Privacy Mask Settings



4. Click and drag the mouse in the live video window to draw the mask area. You are allowed to draw up to 4 areas on the same image.
5. (Optional) click Clear All to clear all of the areas you set without saving them.
6. Click **Save** to save the settings.

Configuring and Handling Alarms

This section explains how to configure the network camera to respond to alarm events, including motion detection, video tampering, alarm input, alarm output and exception. These events can trigger the alarm actions, such as Notify Surveillance Center, Send Email, Trigger Alarm Output, etc.

Note: Check the checkbox of Notify Surveillance Center if you want the alarm information pushed to your mobile phone as soon as the alarm is triggered.

Configuring Motion Detection

Motion detection is a feature which can take alarm response actions and record the video for the motion occurred in the surveillance scene.

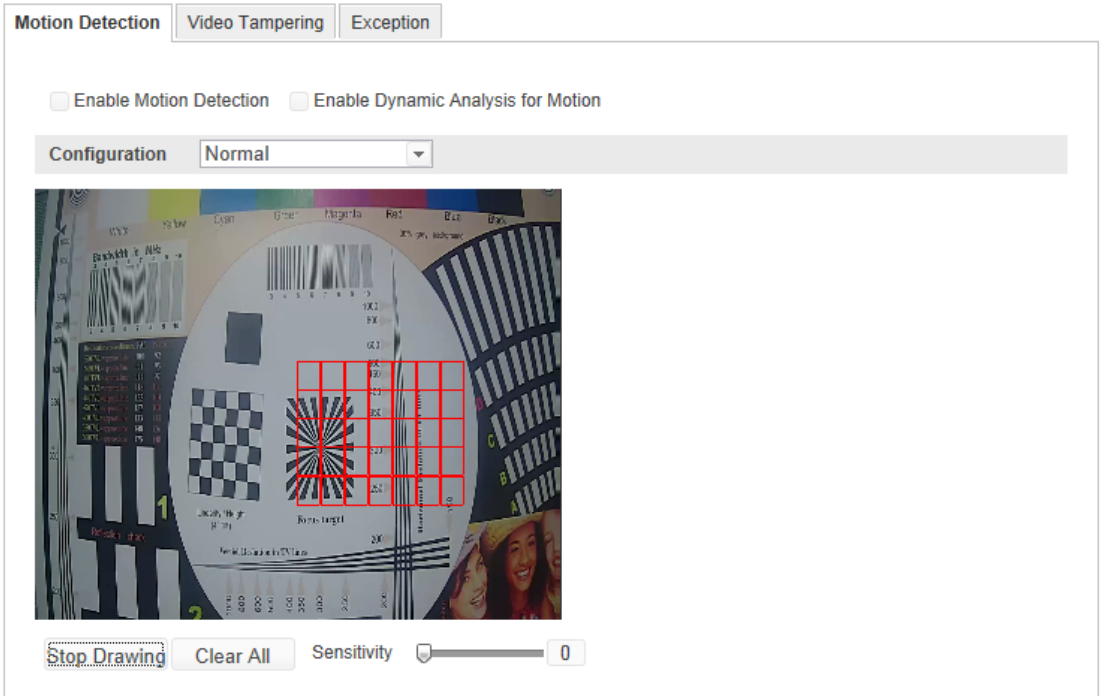
Set the Motion Detection Area.

1. Enter the motion detection settings interface

Configuration> Advanced Configuration> Events > Motion Detection

2. Check the checkbox of Enable Motion Detection.

Figure 37: Enable Motion Detection



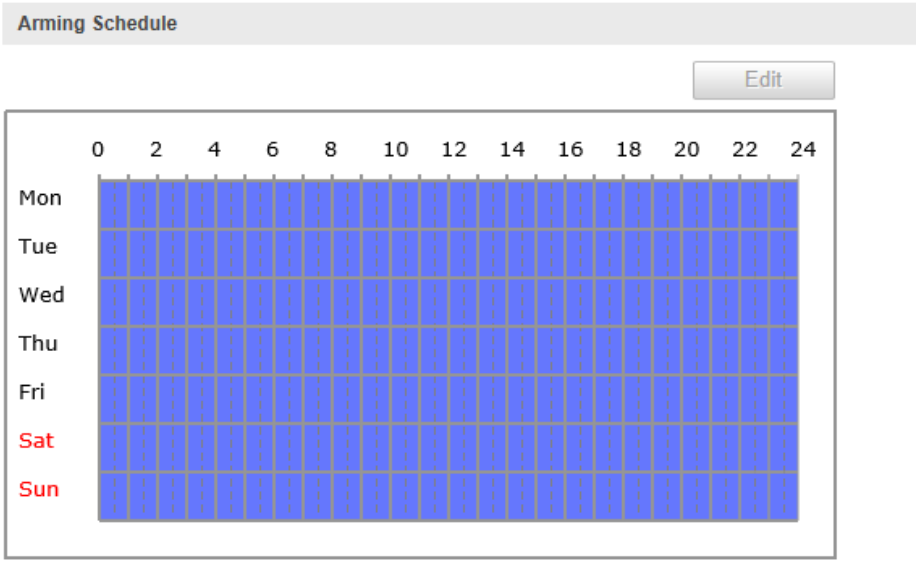
3. Click Draw Area. Click and drag the mouse on the live video image to draw a motion detection area.

   Note: You can draw up to 8 motion detection areas on the same image.

4. Click Stop Drawing to finish drawing.
5. Click Clear All to clear all of the areas.
6. (Optional) Move the slider Sensitivity 0 to set the sensitivity of the detection.

Set the Arming Schedule for Motion Detection.

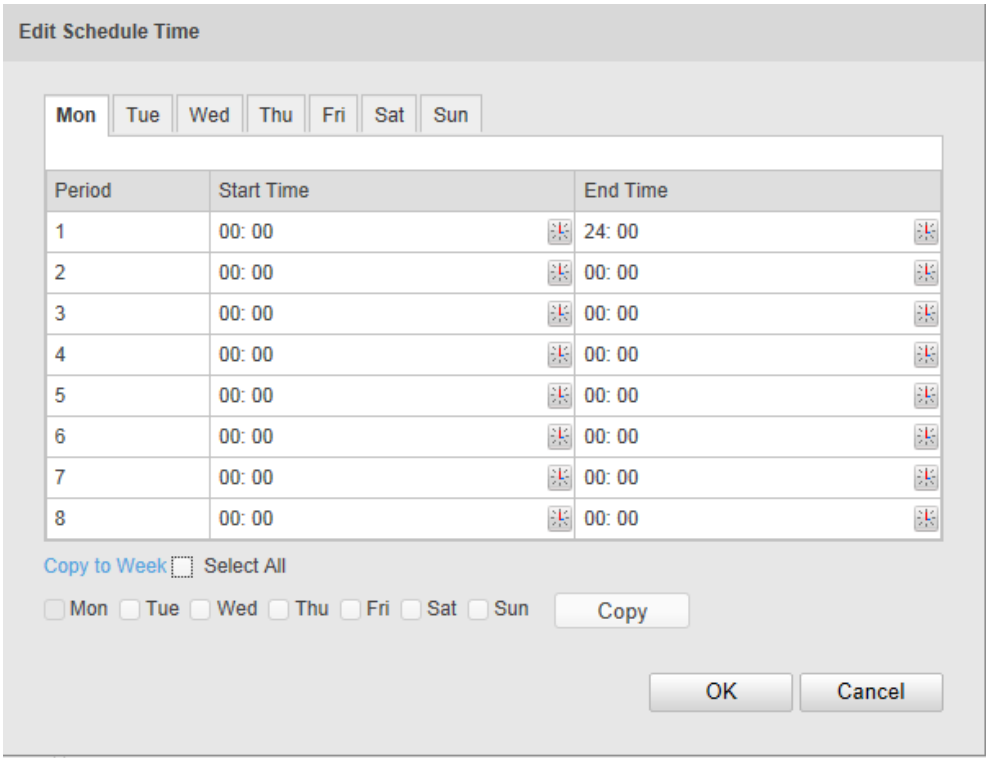
Figure 38: Arming Time



1. Click Edit to edit the arming schedule. The Arming Schedule shows the editing interface of the arming schedule.
2. Choose the day you want to set the arming schedule.
3. Click to set the time period for the arming schedule.
4. After you set the arming schedule, you can copy the schedule to other days.
5. Click **Save** to save the settings.

Note: The time of each period can't be overlapped. Up to 8 periods can be configured for each day.

Figure 39: Arming Time Schedule



Set the Alarm Actions for Motion Detection.

You can specify the linkage method when an event occurs – note that "Linkage" is another way of saying "Notification." This section describes how to configure the different linkage methods.

Figure 40: Linkage Method

1. Check the checkbox to select the linkage method. Notify surveillance center, send email and upload to FTP are selectable (Optional).

   Notify Surveillance Center

   Send an exception or alarm signal to remote management software when an

event occurs.

Send Email

Send an email with alarm information to a user or users when an event occurs.

To send the Email when an event occurs, you need to refer to *Section 0* to set the related parameters.

Upload to FTP

Capture the image when an alarm is triggered and upload the picture to a FTP server.

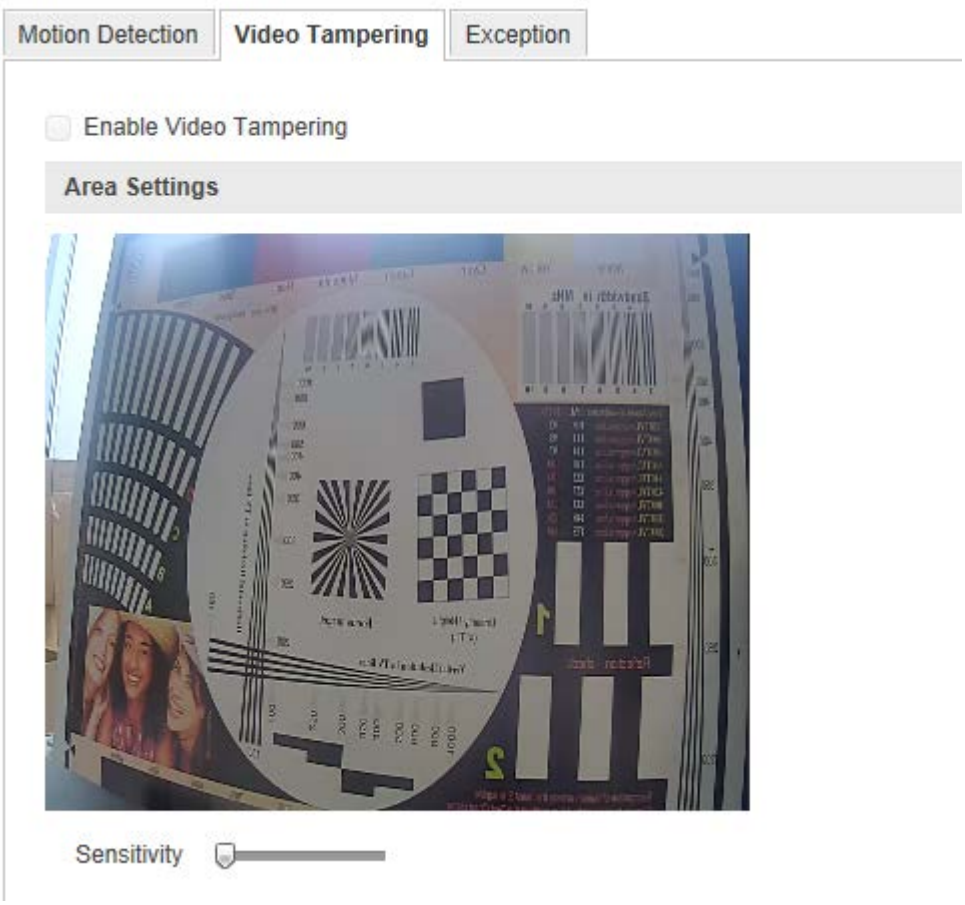
Note: Set the FTP address and the remote FTP server first.

Configuring Video Tampering Alarm

You can configure the camera to trigger the alarm when the lens is covered and take alarm response action.

1. Enter the Video Tampering Settings interface:
   Configuration> Advanced Configuration > Events > Video Tampering

Figure 41: Video Tampering Alarm



2. Check **Enable Video Tampering** checkbox to enable the video tampering detection.
3. Click Edit to edit the arming schedule for video tampering. The arming schedule configuration is the same as the setting of the arming schedule for motion detection.
4. Check the checkbox to select the linkage method taken for the video tampering. Audible warning, notify surveillance center, send email and trigger alarm output are selectable.
5. Click **Save** to save the settings.

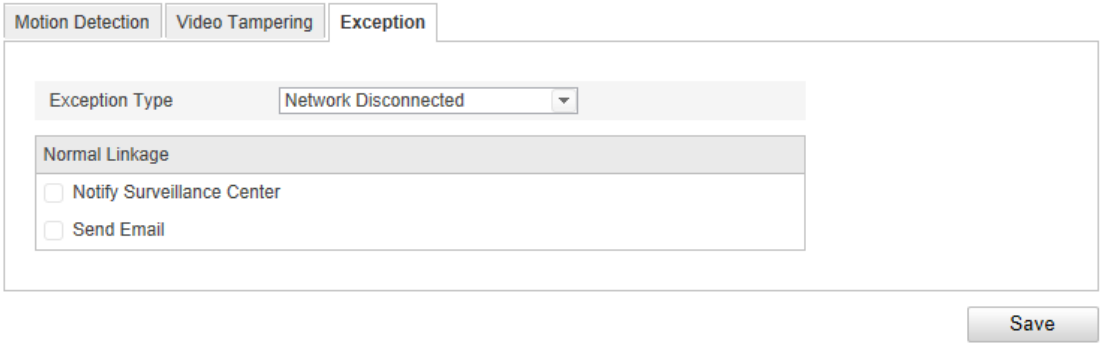
Handling Exception

The exception type can be Network Disconnected, IP Address Conflicted, and Illegal Login to the cameras.

1. Enter the Exception Settings interface:
Configuration> Advanced Configuration> Events > Exception
2. Check the checkbox to set the actions taken for the Exception alarm. Refer to

Set the Alarm Actions Taken for Motion Detection

Figure 42: Exception Settings



3. Click **Save** to save the settings.

Others

Managing User Accounts

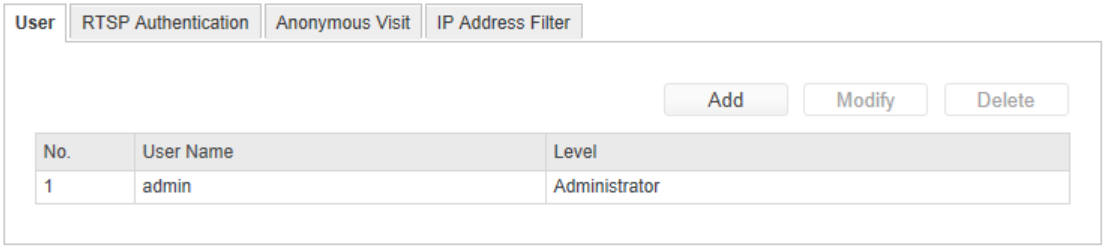
Enter the User Management interface:

Configuration> Basic Configuration> Security > User

Or Configuration > Advanced Configuration> Security > User

The **admin** user has access to create, modify or delete other accounts. Up to 15 user accounts can be created.

Figure 43: User Information



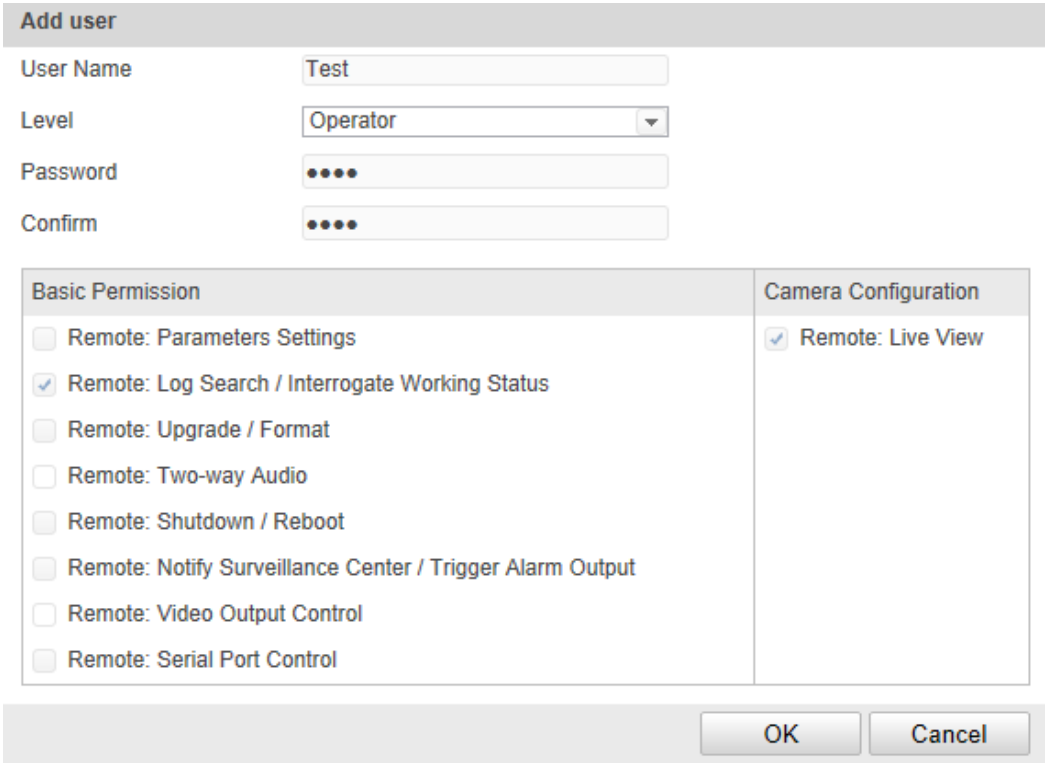
Add a User

1. Click Add to add a user.
2. Input the new **User Name**, select **Level** and input **Password.**

Note: The level indicates the permissions you give to the user. You can define the user as **Operator** or **User**.

3. In the **Basic Permission** field and **Camera Configuration** field, you can check or uncheck the permissions for the new user.
4. Click OK to finish the user addition.

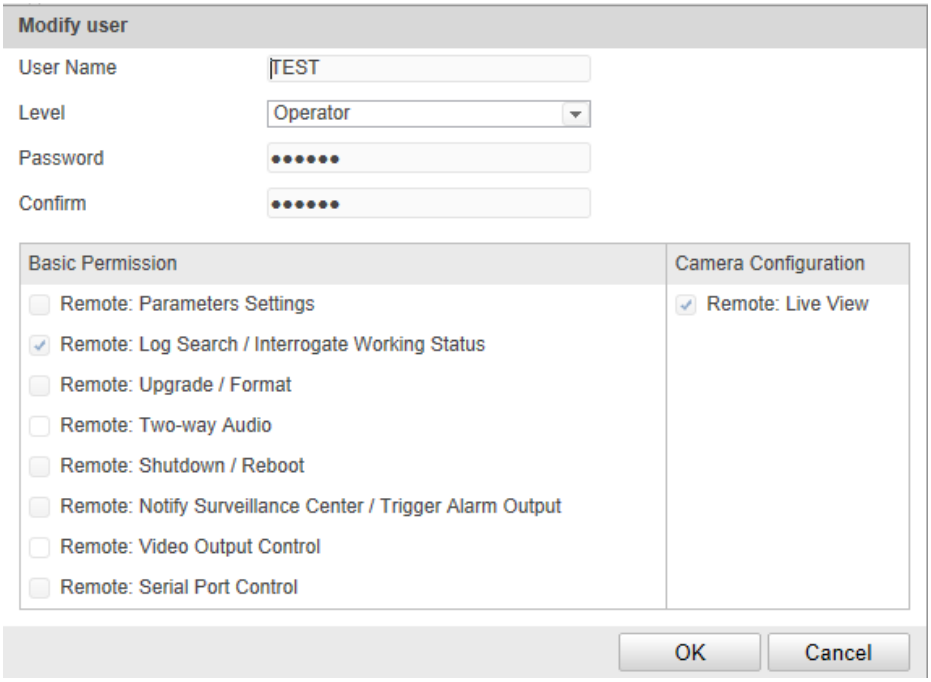
Figure 44: Add a User



Modify a User

1. Left-click to select the user from the list and click Modify.
2. Modify the **User Name**, **Level** or **Password**.
3. In the **Basic Permission** field and **Camera Configuration** field, you can check or uncheck the permissions.
4. Click **OK** to finish the user modification.

Figure 45: Modify a User



Delete a User

1. Select the user you want to delete, and click Delete.
2. Click OK when dialogue box pops up to confirm the operation.

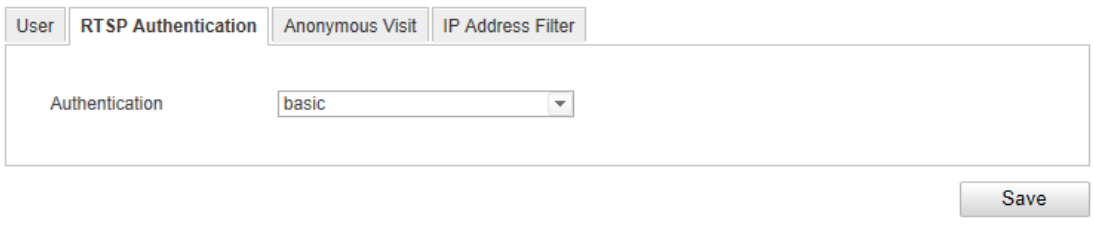
Configuring RTSP Authentication

You can specifically secure the stream data of live view.

1. Enter the RTSP Authentication interface**:**

Configuration> Advanced Configuration> Security > RTSP Authentication

Figure 46: RTSP Authentication



2. Select the **Authentication** type **basic** or **disable** in the drop-down list to

enable or disable the RTSP authentication.

Note: If you disable the RTSP authentication, anyone can access the video stream by the RTSP protocol via the IP address.

3. Click **Save** to save the settings.

Anonymous Visit

Enabling this function allows visits by users who do not have the user name and password of the device.

1. Enter the Anonymous Visit interface:

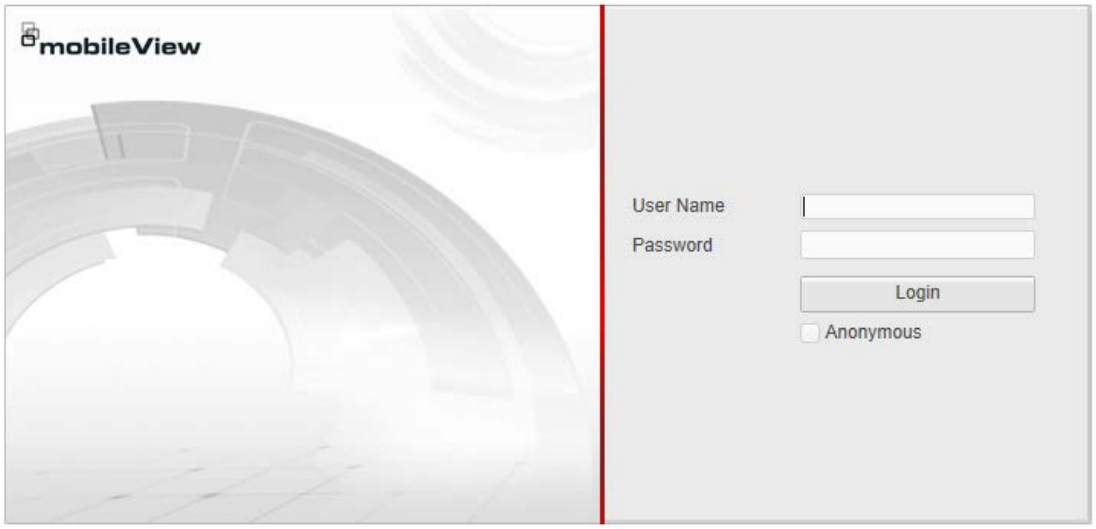
Configuration> Advanced Configuration> Security > Anonymous Visit

Figure 47: Anonymous Visit

2. Set the **Anonymous Visit** permission **Enable** or **Disable** in the drop-down list to enable or disable anonymous visits.
3. Click **Save** to save the settings.

   There will be a checkbox of Anonymous the next time you log in.

Figure 48: Login Interface with Anonymous checkbox



4. Check the checkbox of **Anonymous** and click **Login**.

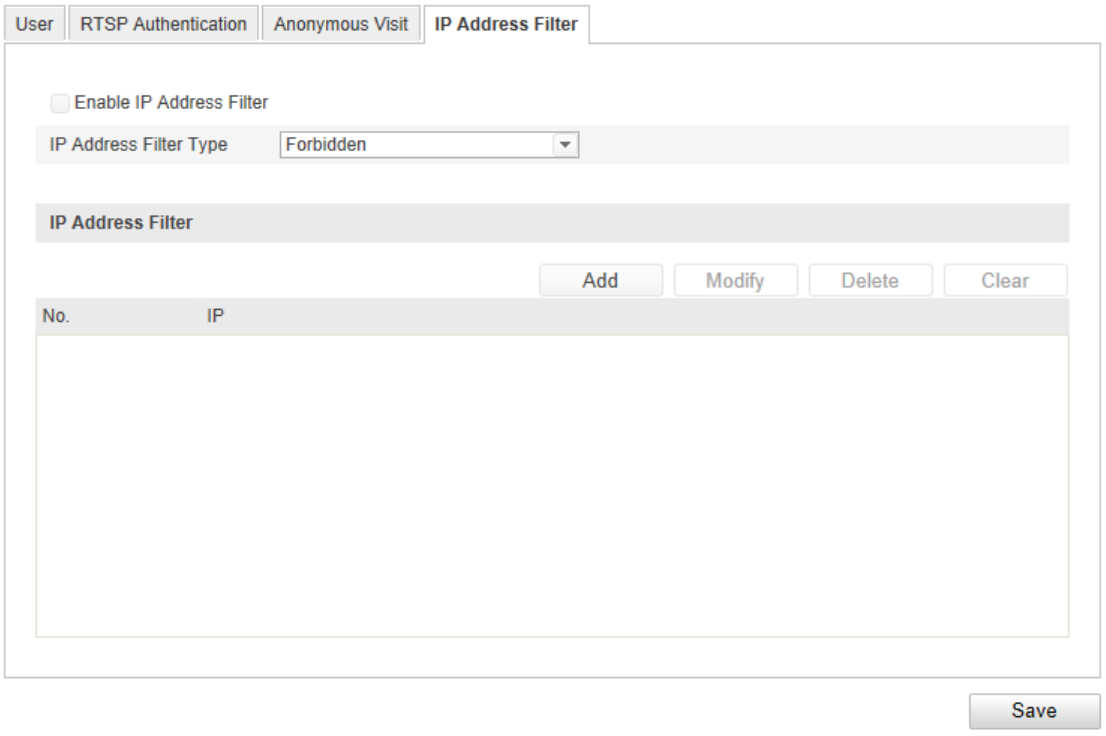
IP Address Filter

This function makes it possible for access control.

1. Enter the IP Address Filter interface:

Configuration> Advanced Configuration> Security > IP Address Filter

Figure 49: IP Address Filter Interface

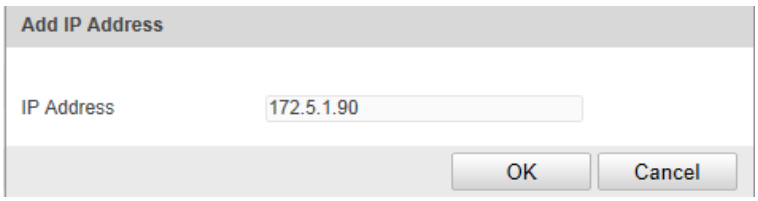


2. Check the checkbox of **Enable IP Address Filter**.
3. Select the type of IP Address Filter in the drop-down list, **Forbidden** and **Allowed** are selectable.
4. Set the IP Address Filter list.

   Add an IP Address

   - Click Add to add an IP.
   - Input the IP Adreess.

Figure 50: Add an IP

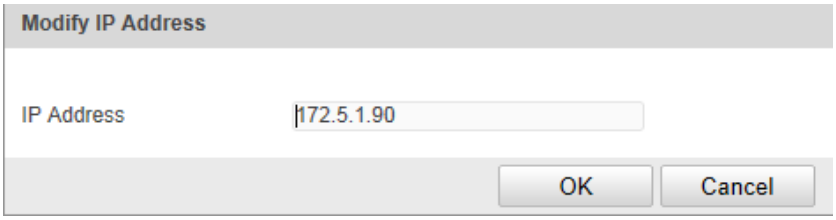


- Click OK to finish adding.

Modify an IP Address

- Left-click an IP address from filter list and click Modify.
- Modify the IP address in the text filed.

Figure 51: Modify an IP



- Click the OK button to finish modification.

Delete an IP Address

- Left-click an IP address from filter list and click Delete.

Delete all IP Addresses

- Click Clear to delete all the IP addresses.

5. Click **Save** to save the settings.

Viewing Device Information

Enter the Device Information interface:

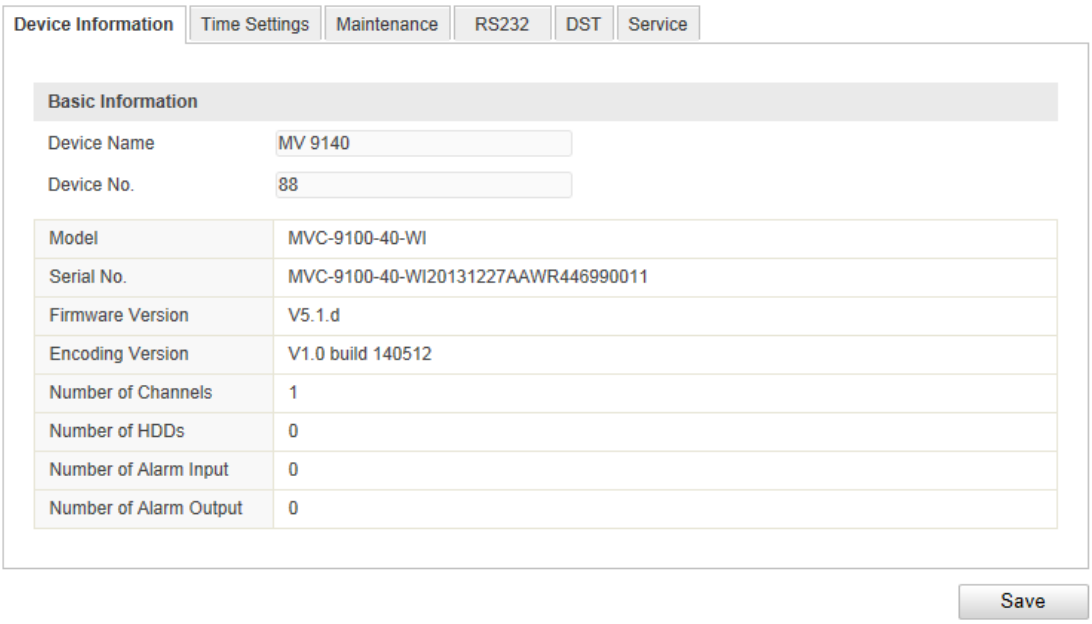
Configuration> Basic Configuration> System > Device Information

Or **Configuration > Advanced Configuration> System > Device Information**

In the **Device Information** interface, you can edit the Device Name.

Other information of the network camera, such as Model, Serial No., Firmware Version, Encoding Version, Number of Channels, Number of HDDs, Number of Alarm Inputs and Number of Alarm Outputs are displayed. The information cannot be changed in this menu. It is the reference for maintenance or modification in future.

Figure 52: Device Information



Maintenance

Rebooting the Camera

1. Enter the Maintenance interface:

Configuration> Basic Configuration> System > Maintenance

Or **Configuration > Advanced Configuration> System > Maintenance:**

2. Click **Reboot** to reboot the camera.

Figure 53: Reboot the Device

Restoring Default Settings

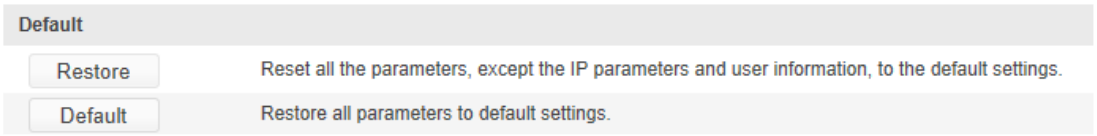
1. Enter the Maintenance interface:

Configuration> Basic Configuration> System > Maintenance

Or **Configuration > Advanced Configuration> System > Maintenance**

2. Click **Restore** or **Default** to restore the default settings.

Figure 54: Restore Default Settings



Note: After restoring the default settings, the IP address is also restored to the default IP address, please be careful with this action.

Exporting/ Importing Configuration File

Enter the Maintenance interface:

Configuration> Basic Configuration> System > Maintenance

Or **Configuration > Advanced Configuration> System > Maintenance**

1. Click **Export** to save the configuration file of the current device.
2. Click **Browse** to select the saved configuration file and then click **Import** to start importing configuration file.
3. Click **Reboot** to reboot the camera.

Upgrading the Camera Firmware

1. Enter the Maintenance interface:

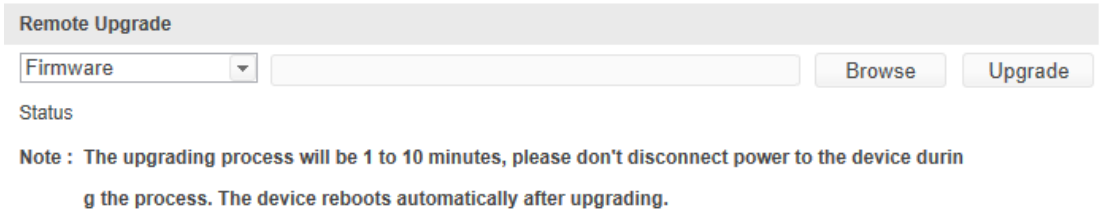
   Configuration> Basic Configuration> System > Maintenance

   or **Configuration > Advanced Configuration> System > Maintenance**

2. Click **Browse** to select the local upgrade file and then click **Upgrade** to start the upgrade.

Note: The upgrading process will take 1 to 10 minutes. Please don't disconnect power of the camera during the process. The camera reboots automatically after upgrading. To ensure your browser displays updated camera menus, you may need to clear/delete the website history in your browser after the camera reboots.

Figure 55: Remote Upgrade



RS-232 Settings

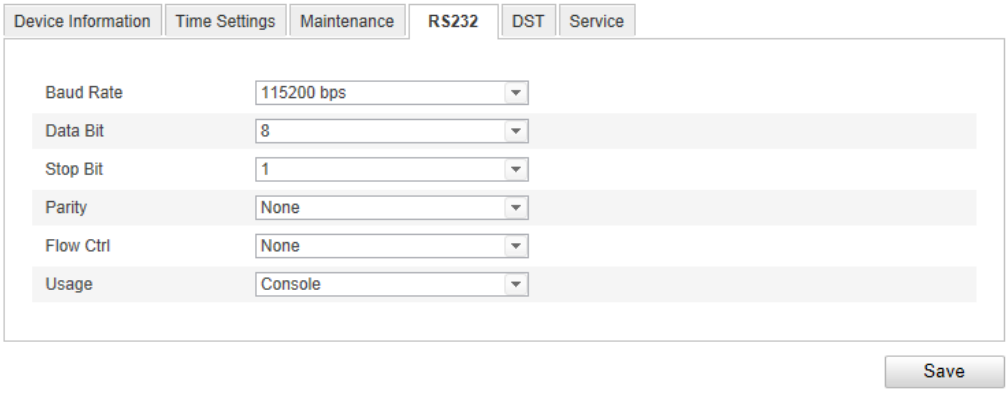
The RS-232 port can be used in two ways:

- Parameters Configuration: Connect a computer to the camera through the serial port. Device parameters can be configured by using software such as HyperTerminal. The serial port parameters must be the same as the serial port parameters of the camera.
- Transparent Channel: Connect a serial device directly to the camera. The serial device will be controlled remotely by the computer through the network.

1. Enter RS-232 Port Setting interface:

   Configuration> Advanced Configuration> System > RS232

Figure 56: RS-232 Settings



Note: If you want to connect the camera by the RS-232 port, the parameters of the RS-232 should be exactly the same with the parameters you configured here.

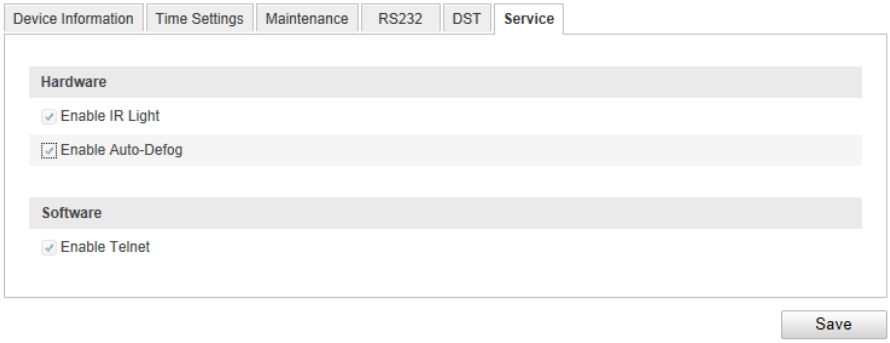
2. Click **Save** to save the settings.

Defog Settings (only available on MVC-9000)

User can check the defog option to enable the heater. If the temperature is below 25C, the heater will be on; when temperature exceeds 25C, the heater will be off.

1. Enter Defog Setting interface:

   Configuration> Advanced Configuration> System > Service



2. Click **Save** to save the settings.

IR Settings

User can check the IR option to enable or disable IR LED.

1. Enter IR Light interface:

   Configuration> Advanced Configuration> System > Service

2. Check the checkbox to enable IR LED.
3. Click **Save** to save the settings.

Telnet Settings

To enable or disable Telnet do the following:

1. Enter Telnet interface:

   Configuration> Advanced Configuration> System > Service

2. Check the checkbox to enable Telnet.
3. Click **Save** to save the setting.